

Anno 2 - N. 40
18 Dicembre 2003- 1 Gennaio 2004

**Direttore Responsabile:** Luca Sprea

**I Ragazzi della redazione europea:**
grand@hackerjournal.it, Il Coccia, Gualtiero Bismark.it, Tronconi, Ana Esteban, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron

**Service:** Cometa s.a.s.

**DTP:** Cesare Salgaro

**Graphic designer:** Dopla Graphic S.r.l.
info@dopla.com

**Copertina:** Daniele Festa

**Publishing company**
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

**Printing**
Roto 2000

**Distributore**
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

**Abbonamenti**
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.



**HJ: INTASATE LE NOSTRE CASELLE**

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. **redazione@hackerjournal.it**

**hack·er (hãk'∂r)**

***"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."***

## LUCY IN THE SKY WITH FUNCARD

Per chi fosse di ritorno ora da un viaggio sulla Stazione Spaziale Internazionale (http://spaceflight.nasa.gov/station), da qualche tempo nel panorama della TV satellitare italiana è arrivata la Sky di Rupert Murdoch a prendere il posto di Tele+ e compagnia.

Contemporaneamente nei forum e nei newsgroup è scoppiato un bel pandemonio. Se prima lo sport preferito degli italiani-con-parabola era trovare il modo di guardarsi le partite a scrocco o ridiffondere per tutto il condominio il segnale di un singolo decoder, ora la cuccagna sembra finita. Sky ha sistemi di cifratura più astuti e flessibili, si dice, e piratare le sue card è divenuto impossibile oppure molto meno facile e conveniente di prima, si dice.

Detto che non esista alcuna protezione inviolabile, il problema è trovare un modo semplice e praticabile per violarla e questa sembra essere la situazione attuale. Abbiamo fatto il punto della situazione e anche dato un paio di avvisi ai naviganti più sprovveduti, perché c'è gente che va in giro a millantare credito per estorcere denaro ai gonzi, e là fuori è pieno di gonzi (la prova è che i lettori di Hacker Journal sono decine di migliaia e gli italiani sono decine di milioni. I gonzi sono tutti fuori dal primo insieme e dentro il secondo :-)

Torneremo sull'argomento anche perché tra poco arrivano i decoder digitali terrestri e il tutto diverrà ancora più interessante. È proprio bello vivere in tempi di continue novità tecnologiche!

Come si noterà, abbiamo lavorato a un bel restyling della rivista. Speriamo che piaccia e restiamo in attesa di complimenti e critiche, in modo da creare un Hacker Journal più che mai all'altezza di tutte le aspettative.

Sky non è certo l'unica attrazione di questo numero, peraltro; parliamo di X-box contro Linux, tecniche base di ingegneria sociale, bambine dodicenni condannate a pagare duemila dollari di multa per avere usato un programma peer-to-peer e altro ancora, passando per tutorial e cose di imparare pensate un po' per tutti.

Tra questi ne segnaliamo uno in particolare, quello dedicato a Google. È accessibile a chiunque ma contiene qualche dritta anche per i più bravi. Se c'è uno strumento che sembra veramente universale di questi tempi, è proprio il motore di ricerca, e il motore di ricerca, insomma, è Google.

Buona lettura e sotto con l'hacking!

**Barg the Gnoll**
gnoll@hackerjournal.it

**One4Bus**
one4bus@hackerjournal.it

FREE HACK NET

Saremo di nuovo in edicola Giovedì 1 Gennaio !




La prima rivista hacking italiana

2 € NO PUBBLICITÀ SOLO INFORMAZIONI E ARTICOLI

FREE HACK NET




freeHACKnet è il servizio gratuito di collegamento a Internet targato Hacker Journal: indirizzo email quellochevuoi@hackerjournal.it con 5 Mbyte, accesso super veloce fino a 128 Kbit al secondo (ISDN multilink PPP), server newsgroup, controllo anti virus e anti spam. Niente abbonamento, nessuno sbattimento, paghi solo la tariffa telefonica urbana. Corri subito a iscriverti su

**www.hackerjournal.it/freeinternet**

# Nuova password!

**Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete gli arretrati, informazioni e approfondimenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo!**

**user: fos7**
**pass: cul8**

# I VOSTRI SITI...







Volevo segnalarvi un sito da surfare di cui stiamo parlando sul forum off-topic nel 3d brebei:programmatore fallito, http://brebei.splinder.it. Non è un sito tecnico però fa troppo ridere. **Anemone** *Di mamma ce n'è una sola, ma di virgili evidentemente ce nè più di uno!*




Volevo segnalare il mio sito, http://www.etnuz.tk.
È ancora in aggiornamento,ma
presto sarà completo...siete grandi! **Alberto**
*Grazie! Salutiamo anche noi l'ipsia di Carbonia!*




Vorrei proporre il mio sito per la vostra rivista:
http://www.hackersweb.da.ru. **Andrea**
*C'è già una taglia sulla tua testa? Altro che Kevin Mitnick!*









mailto:
redazione@hackerjournal.it

## MA CHE SISTEMA È?

Il mio firewall rivela nel mio computer un trojan, ma non lo cancella. Dicendomi che è impossibile cancellarlo a causa di un errore. Vorrei sapere da voi se avete un sistema per riparare questo problema.

**Hacker CG**

*Non ci dici che firewall è, che computer è, che trojan è, che errore è e di conseguenza è un po' difficile consigliarti una soluzione, a parte l'essere munito di un buon antivirus sempre aggiornato. In generale, chiedere una risposta a una redazione è come chiederla a un medico: bisogna essere precisi e dettagliati con tutti i sintomi. Come i medici, anche due redattori diversi daranno due risposte diverse a una stessa domanda, ma questo è un altro discorso.*

## PASSWORD DIMENTICATA

Ciao gentile redazione di hackerjournal, sono un vostro lettore dal primo numero, volevo farvi due domande, io ho installato sul mio computer Windows 2000 professional, in due parole mi sono dimenticato la password da amministratore, come faccio per riprenderla? La seconda domanda è: ho visto che ci sono dei key log hardware da attaccare al computer prima della tastiera, mi interessava moltissimo, ma a me serviva una versione con la porta usb, volevo sapere se esisteva e dove potevo aquistarla.
Vi ringrazio molto, ciao,

**AleX_h**

*Ciao Alex!*
*E' sempre meglio porre una domanda per volta alla redazione, che ci mette meno a rispondere ed è quindi più facile che pubblichi la tua lettera. Ma per stavolta facciamo una eccezione.*
*La soluzione semplice al problema della password di amministrazione è entrare nel sistema con un altro account dotato di poteri di amministrazione e cambiare la password dell'utente amministratore che non ricordi più. Le persone sagge tengono sempre sul computer un account di amministrazione, per così dire, di riserva. Se invece hai un account solo sul computer, ecco un'altra soluzione.*
*Quando 2000 parte, mostra la finestra di logon e, nel caso non succeda niente per un po', fa partire il salvaschermo LOGON.SCR. Accedi ai file del tuo computer da un altro computer, e sostituisci il file LOGON.SCR con CMD.EXE. La volta successiva, invece che partire il salvaschermo, parte la console di comando. A quel punto puoi lanciare la console di Computer Management (COMPMGMT.MSC) e cambi la password.*
*La procedura di sostituzione di LOGON.SCR con CMD.EXE dipende dall'uso nel sistema di FAT oppure NTFS. Se usi FAT puoi partire da un disco di boot di Windows 95/98 o da un floppy di boot DOS. Per sistemi NTFS che non siano in rete ti può servire un programma apposito, tipo NFTSDOS.*
*Per il futuro, pensa anche a crearti un CD o un floppy di boot da tenere da parte, che contenga uno strumento in grado di risolvere il problema.*
*In Rete circolano vari software per cavarsela in queste situazioni. Probabilmente uno che fa al caso tuo è NTAccess 1.5, che trovi a http://www.mirider.com/ntaccess.html. Trovi un'altra utility a http://home.eunet.no/~pnordahl/ntpasswd. Per quanto riguarda i key logger hardware, relativamente a Windows abbiamo notizia solo di dispositivi PS/2. Se qualcuno conosce un key logger USB ce lo segnali!*




## LA FONT DEL DESIDERIO

So che potrebbe sembrare una domanda stupida (anzi, lo è), però mi piace tantissimo il font che usate nella rivista...mi potreste dire il nome? Dove posso trovarlo (uso Win98 purtroppo…) visto che non l'ho nel mio computer? Grazie mille! Siete grandi!

**Naqern**




*Non esistono domande stupide! Fino al numero 39 abbiamo usato un font chiamato Futura. Da questo numero in avanti stiamo usando un Helvetica. Puoi trovarli tramite motori di ricerca come http://www.free-fonts-free-fonts.com, ma non illuderti vedendo l'URL: questi sono font commerciali, a pagamento. In compenso potrai trovare un sacco di font gratuiti molto simili e, già che ci siamo, l'Arial che viene installato su Windows dà risultati di stampa abbastanza simili a quelli di Helvetica.*

## REVERSE REVERSE ENGINEERING

Vi scrivo a proposito del reverse engineering [HJ38,], l'argomento mi piace molto ma volevo kiedere se era possibile che pobblicaste un articolo "completo" nel senso ke contenga istruzioni e metodi applicabili a tutti i programmi e appli-

```
Count = 200 (512.)
Buffer = giochino.004031A1
hWnd = [illegible] (class='Edit',parent=[illegible])
GetWindowTextA
String = "Topolino"
lstrlenA

Style = MB_OK|MB_ICONEXCLAMATION|MB_APPLMODAL
Title = "Sbagliato!"
Text = "La risposta NON è corretta![illegible] :-]"
hOwner = NULL
MessageBoxA

ASCII "Topolino"

ASCII "6/66)F6/5'#x/xx/)#"

String2 = "6/66)F6/5'#x/xx/)#"
String1 = "Topolino"
lstrcmpA
```

cazioni in alternativa potreste consigliarmi un sito (in italiano) ke tratti approfonditamente l'argomento, grazie anticipatamente siete mitici continuate così.

**JCD_90**

# www.hackerjournal.it

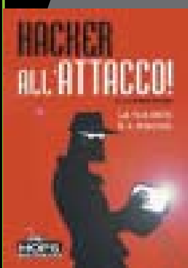


***Un articolo completo sul reverse engineering? Non riusciamo a pubblicare un Hacker Journal da mille pagine... scherzi a parte, il reverse engineering è un argomento letteralmente senza fine e uno di quelli che si impara più facendo che leggendo. Perché non provi a contattare direttamente l'autore dell'articolo? Se hai domande specifiche sarà felice di risponderti.***

## L'ARTE DELL'HACKING

Ciao io sono un ragazzo di 14 anni che adora il computer e ora voglio ampliare le mie conoscenze sul computer, non sapreste consigliarmi un libro per imparare + approfonditamente il computer e l'arte dell'hacking? Vi prego rispondete.

**Angelo**




***Ciao Angelo!***
***Ti consiglio non uno ma due libri: il primo si intitola Hacker all'attacco, il secondo Il manuale del giovane hacker (seconda edizione). Sono entrambi editi da Hops Libri (http://www.hopslibri.com). Il primo è già in libreria, il secondo dovrebbe essere disponibile nel momento in cui leggi questa risposta.***
***Se entri nel nostro sito scoprirai come poterli ordinare online e avere uno sconto del 15% sul prezzo di copertina.***

## TUTTO QUI? :-)

Sono (come dire) un aspirante Hacker. [complimenti] Ah,spero che publichiate questa mia e-mail nello spazio apposito della vostra rivista,mi fareste davvero molto felice. [complimenti]

**Lordhark**

***Non ti offenderai se lasciamo da parte i complimenti, che si devono sempre meritare, ma che sono sempre estremamente apprezzati (le critiche le pubblichiamo, invece!). Ecco la tua e-mail e grazie mille per l'augurio con utilizzo di balena. :-)***

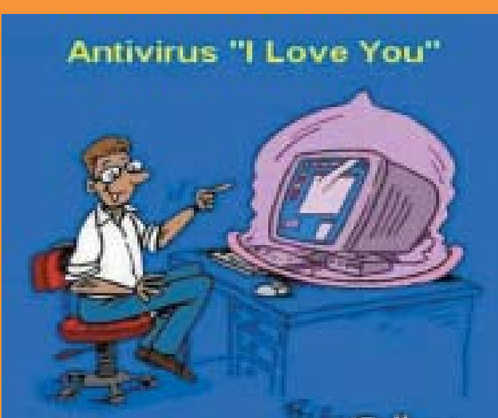
## AL FIN DELLA LICENZA

Cara redazione,
sto lavorando alla realizzazione di un progetto in cui tutti possano pubblicare i propri libri e racconti di qualsiasi genere essi siano, spaziando dalla letteratura all'informatica. Per fare questo c'è bisogno di una licenza che tuteli quelli scritti…
Cosa devo fare?
Grazie in anticipo

**phj**

***Caro phj,***
***a meno che gli autori non rinuncino volontariamente al loro copyright usando licenze tipo copyleft (consulta http://www.gnu.org/copyleft/copyleft.html per informazioni più dettagliate), per il solo fatto di essere pubblicati i loro contenuti sono protetti da copyright. Il difficile è accorgersi delle violazioni del copyright e qui non è questione di licenze, ma di risorse.***

### Tech Humor




### Tech Humor




## ALLA RICERCA DEL COMPILATORE PERDUTO

Frequento il primo anno di informatica… ho un esame sull'assembler ma non riesco a trovare un compilatore o cmq un programma che mi faccia il debug e esegua i file che ho creato… ma per Linux sapete dove posso trovarlo in rete?

**enrico —baru—**

***Non dici che assembler vuoi però! Se ti serve per processori Intel, prova nasm. Lo trovi a http://rpmfind.net/linux/RPM/PLD/dists/ac/Development_Tools.html.***

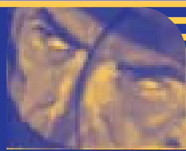
## DTITFM?

Gentile redazione, non vi annoierò con le solite frasi fatte di complimenti [grazie per i complimenti e grazie per la sintesi allora!]. Vengo al dunque: da non molto ho cominciato a muovere i primi passi con la "scatola nera" con la quale vi sto scrivendo. Affascinato da quanto asserite nella Vs rivista di linux sono corso in edicola a comperare una versione dello stesso ma dopo averlo installato sono cominciati i problemi. Nella Vs. rivista leggevo che uno dei consigli più frequenti è RTFM ovvero leggetevi il fottuto manuale. Ciò detto pongo la domanda: ma dove lo trovo il fottuto manuale se giro nelle varie edicole e vi è sempre una copia del programma ma mai la copia del manuale? Vivo in Roma se avete un indirizzo utile datemelo. Grazie.




**Raffaele Scognamiglio**

***Gentile Raffaele,***
***quando installi Linux da una distribuzione su CD i CD stessi sono pieni di documentazione e in generale ogni programma ha un suo manuale. Per gli strumenti di shell hai a disposizione il comando man comando e inoltre si trova una imponente massa di documentazione in Rete. In particolare potresti dare un'occhiata all'Italian Linux Documentation Project, a http://ildp.pluto.linux.it.***



NEWS

## CARTE D'IDENTITÀ BIOMETRICHE: INUTILI?

Il Regno Unito sta pensando di introdurre carte di identità biometriche che riportano dati considerati praticamente non falsificabili, come scansioni della retina e altro. Tuttavia le analisi della London School of Economics mostrano come il sistema progettato non fermerà i criminali intenzionati a procurarsi più carte sotto nomi diversi. In più la scansione della retina è un procedimento ancora troppo soggetto a fattori ambientali, tanto che il riconoscimento ha una precisione del 99 percento. Sembra molto alta e invece, su database enormi come quelli di una popolazione nazionale (si pensi all'Italiam con 60 milioni di abitanti) è una percentuale disastrosamente bassa, che arrecherebbe grandi fastidi a cittadini onesti e aumenterebbe le probabilità che un criminale la faccia franca. Si stanno studiando soluzioni come quella di includere nella carta sia la scansione retinica sia l'impronta digitale. La precisione aumenterebbe di molto, ma così anche i costi.

---------------------------------------

## SCRIVI, SCRIVI, CHE TI PARAFRASO

Tutti i giorni riformuliamo un sacco di volte il nostro pensiero, per rispiegare una cosa che il nostro interlocutore non ha capito, oppure per portare un attacco vincente di ingegneria sociale verso un ignaro impiegato dei telefoni o delle poste. Questa è una cosa che da sempre ci distingue rispetto ai computer, incapaci di parafrasare alcunché.
Le cose però iniziano a cambiare. Un team di ricercatori della Cornell University ha mutuato procedure tipiche del giornalismo online, le ha incrociate con schemi di analisi tipici della bioinformatica ed è arrivato a progressi sostanziali in materia.
In pratica i ricercatori hanno studiato come più persone esprimono in parole diverse lo stesso concetto e hanno confrontato i vari modi di espressione con tecniche usate normalmente per confrontare tra loro i geni che albergano nel DNA.
Dopo Google News, che raccoglie le notizie automaticamente, sta arrivando dunque il redattore elettronico, capace di riassumere e rielaborare le notizie da solo. Mi sa che nel 2015 Hacker Journal lo scriverà un computer Linux, tutto da solo. O no?

## 29 NOVEMBRE: VIVA IL SOFTWARE LIBERO!






Grande attività e tanti incontri in tutta Italia per la giornata nazionale del software libero, celebrata sabato 29 novembre scorso. Non abbiamo lo spazio per raccontare tutto ora (qualcuno ha voglia di rassumerci le sue esperienze personali?) ma di città in città si sono moltiplicate le iniziative di ogni genere di associazioni. Dopo i 40 Comuni coinvolti dell'edizione 2001 e i 60 del 2002, si può solo parlare di ennesimo record. Per fare solo qualche esempio, a Milano il Laboratorio Innovazione Breda ha visto oltre mille visitatori. A Firenze l'incontro è stato dedicato al software libero nei Paesi in via di sviluppo, organizzato dal Firenze Linux User Group. A Trento si è parlato di tutto, dalle distribuzioni più recenti alle esperienze dei nuovi arrivati. A Crema si parlato di tutto, dalle sottigliezze tecniche del kernel fino al rapporto tra Linux e videogiochi. E così via. Attendiamo i resoconti da tutta Italia per dare loro il massimo spazio possibile su Hj!

http://milano.linux.it
http://www.firenze.linux.it
http://www.linuxtrent.it
http://carapax.crema.unimi.it/eventi/ld2003/ld2003.php

## FINE DI (ALMENO UN) DIALER



Ha fatto la fine che si meritava il finto notiziario Inforete, che con la scusa delle news in realtà portava a un dialer per spillare soldi ai navigatori più ingenui dall'indrizzo http://members.yodahosting.com/inforete. Di dialer ce ne sono milioni ma questo aveva veramente esagerato, copiando informazioni da Punto Informatico per sembrare più attendibile. Se il pericolo esisteva solo per chi usa Windows insieme a Internet Explorer (la combinazione più esposta a dialer e vari altri tipi di codice ostile presente sul Web), è comunque confortante sapere che il sito è stato disattivato. In questo momento all'URL si può vedere un commento poco gentile di "hacker poco pazienti" e niente più. bene così.

**Attacco portato da hackers non pazienti**

The Doc on The Rock.

## UN ALBERO DA HACKER



È Natale per tutti, anche per chi vede le cose con occhio diverso dagli altri e inventa utilizzi nuovi per le cose vecchie: come dire un hacker.
E allora, chi più hacker di Pietro Cucchi, imprenditore di Bussero (alle porte di Milano), che ha voluto un albero di Natale artificiale alto oltre cento metri, addobbato da non meno di 237 mila lampadine.
A metà tra l'attrazione turistica e il capolavoro postmoderno, l'albero è sostenuto da una struttura esagonale in acciaio del peso di oltre quindici tonnellate. Le luci sono gestite da un software apposito che crea combinazioni di luci sempre nuove.
Se passate da Bussero, in via Genova 2, avete tempo fino al 16 gennaio 2004 per vederlo dal vivo. Nel frattempo consideratelo come un piccolo grande augurio di Natale per tutti i lettori di Hacker Journal e, già che ci siamo, anche Hackers Magazine.






## GLI USA DI NUOVO VERSO LA LUNA?

Da anni il programma spaziale americano procede ma ha perso molto dello spunto iniziale che ha portato Neil Armstrong a sbarcare per primo sul nostro satellite. Problemi finanziari, incidenti mortali alle navette Challenger e Columbia e scarsa efficienza di molti enti hanno infatti ridotto le aspettative e le prospettive dei programmi spaziali della NASA.
Tutto questo potrebbe però cambiare il 17 dicembre, quando il presidente George W. Bush terrà un discorso in occasione del centenario del primo volo umano a bordo di un mezzo più pesante dell'aria. Secondo molti, infatti, Dubya (il nickname di Bush figlio) sceglierà proprio quell'occasione per rilanciare il sogno della conquista spaziale, finito in soffitta da oltre trent'anni. Dopo l'epico sbarco del 21 luglio 1969, infatti, le missioni lunari hanno avuto luogo fino a dicembre 1972, per poi terminare.
A oggi più di 125 milioni di americani sono nati dopo che l'ultimo uomo ha posato l'ultimo piede sulla Luna.
Violare i computer della NASA potrebbe tornare a essere uno degli sport preferiti degli hacker più intraprendenti.



**La Luna, come in questa foto spettacolare, si è eclissata. Ma forse ci torneremo.**

## HP SI SVEGLIA SULLA MUSICA ONLINE

Hewlett-Packard si è improvvisamente svegliata da un lungo sonno e ha deciso di lanciare un negozio online di musica entro il primo trimestre del 2004. Secondo Peter Appl, amministratore delegato di HPShopping.com, il servizio di vendita online avverrà in collaborazione con un'iniziativa già esistente, come Musicmatch.com.
Inoltre la società lancerà sul mercato un riproduttore portatile di musica digitale.
HP è il secondo produttore mondiale di computer dopo Dell, ma sulla musica online è come se fosse ultima. Il mercato, infatti, è dominato dall'iTunes Music Store di Apple (che si dice arriverà a maggio anche in Europa) e dall'analogo servizio di Dell, con dietro numerosa concorrenza che arranca. Al tempo stesso, Apple con il suo iPod e Dell con il suo Digital Jukebox, alias DJ, dominano qualsiasi classifica di vendita di player musicali da taschino.
HP è grande; magari ha anche qualche grande idea per scalzare i numeri uno attuali. Sarà meglio che sia così, perché anche l'idea giusta fa un sacco di fatica i più quando è messa in atto nei tempi sbagliati.




## UN PUZZLE DA VERI HACKER

Mille pezzi, cinquemila pezzi, settemila pezzi sono roba da niente.
Pensate a un puzzle dove i pezzi hanno tutti forma uguale e ci sono miliardi di incastri possibili ma una sola soluzione corretta.
È il principio dello Shmuzzle, gioco inventato da tale Sam Savage, già docente di Management Science alla Università di Chicago. Savage ha avuto l'idea osservando alcune opere di Maurits Cornelis Escher, artista olandese morto nel 1972 e autore di lavori che nascondono trame geometriche assai intricate e paradossi della prospettiva che lasciano interdetti.Escher era un maestro della tassellatura, l'arte di riempire completamente un piano con figure che si incastrano l'una nell'altra all'infinito, senza lasciare spazi vuoti.
E da un'opera di Escher intitolata Reptiles è nata l'idea di creare un puzzle dove lo scopo è sempre quello di comporre il disegno, ma i pezzi hanno tutti forma uguale.
Invitiamo tutti a fare un salto su http://www.shmuzzles.com, dove è anche possibile provare l'ebbrezza di un puzzle davvero impossibile direttamente da browser.
Il vero hacker si fermerà anche a considerare i principi geometrici che stanno dietro al lavoro, magari aiutandosi con http://www.shmuzzles.com/formula.htm.

NEWS

## MAI PIÙ SEDIE A ROTELLE

All'università Waseda di Tokyo, in collaborazione con la produttrice di robot Tmsuk, i ricercatori hanno messo a punto un prototipo di robot capace di camminare su due gambe meccaniche e contemporaneamente trasportare una persona seduta. Si può immaginare come un progresso di questo tipo spalanchi la porta a un futuro assai più confortevole per i disabili e gli ammalati. Il prototipo si chiama WL-16, è alimentato a batterie e riesce a spostarsi in avanti, all'indietro e lateralmente reggendo un adulto del peso massimo, per ora, di sessanta chili. Secondo Yoichi Takamoto, amministratore delegato di Tsmuk, per arrivare a un modello realizzabile in serie ci vorranno "almeno due anni". Nel frattempo, però, il robot è già capace di mantenere l'equilibrio quando il suo carico umano si sposta e riesce a fare passi lunghi trenta centimetri. Prossimi obiettivi: renderlo capace di fare le scale (per ora il gradino massimo superabile è alto pochi millimetri) e passare dall'attuale radiocomando a un joystick montato a bordo, utilizzabile dal passeggero.

---

## SUN ATTACCCA MICROSOFT CON JAVA LOW-COST SU LINUX

Nell'intento di togliere quote di mercato a Windows nel mondo aziendale, Sun ha abbassato il prezzo del suo Java Enterprise System a 50 dollari l'anno per utenza e ha portato Java Desktop System, che consente di collegarsi a un ambiente Windows da una interfaccia interamente basata su Linux con Star Office e Ximian, a 25 dollari per utenza per anno, il tutto fino a metà 2004.La mossa segue il successo conseguito da Sun in Cina, dove un accordo con China Standard Company, azienda controllata dal governo cinese, apre la strada letteralmente a centinaia di milioni di computer sui quali verrà installato Java Desktop System e non Windows.

# NEWS

## NEWS

## CISCO VULNERABILE SUL WI-FI

Cisco, monopolista di fatto del mercato dei router, ha ammesso recentemente una vulnerabilità nella sua linea di punti di accesso wireless Aironet che può consentire ad aggressori ben motivati di accedere a una rete aziendale e curiosare oltre il lecito. Il problema sta nelle chiavi di cifratura, che vengono trasmesse in modo wireless e in testo non cifrato: quindi chiunque, dotato di un computer e dell'antenna giusta, può intercettare le chiavi stesse. una volta che un aggressore è in possesso delle chiavi, qualunque cifratura è inutile per proteggere i dati.



La vulnerabilità affligge i modelli delle serie 1100, 1200 e 1400 con software Cisco IOS 12.2(8)JA, 12.2(11)JA e 12.2(11)JA1. Gli amministratori di rete possono risolverla, tra l'altro, aggiornando a IOS versione 12.2(13)JA1 o successivo. Certo che se gli aggiornamenti fossero numerati in modo più umano anche le vulnerabilità avrebbero vita più difficile!
http://www.cisco.com/warp/public/707/cisco-sa-20031202-SNMP-trap.shtml

---

## UN HOTSPOT IN OGNI BIBLIOTECA… MA IN INGHILTERRA

Il ministro inglese Stephen Timms ha aperto il lavori di un convegno su Wi-Fi & 3G confermando che va avanti il piano di installazione di un punto di accesso wireless in ogni biblioteca pubblica del Regno Unito, annunciato lo scorso settembre. Si spera che i nostri governanti, se non sanno fare meglio, almeno siano in grado di scimmiottare i colleghi britannici.

## VELOCE COME LA LUCE

Da Israele proviene il processore più veloce del mondo, che sfrutta la luce invece della corrente elettrica (www.lenslet.com). Il che significa che è capace di elaborare qualcosa come 8 mila miliardi di operazioni ogni secondo (8 TeraOPS), stracciando di oltre mille volte in velocità qualunque altro dispositivo di elaborazione dei segnali attualmente in commercio.
Il responsabile della Ricerca e Sviluppo del Ministero della Difesa dell'esercito israeliano ha affermato che "Un tale salto quantico nelle prestazioni computazionali, dovuto all'elaborazione ottica, apre nuove possibilità negli scenari militari del futuro, con rilevanti implicazioni strategiche. Questo nuovo sviluppo rivoluzionerà la natura stessa del modo di fare guerra, con effetti simili a quelli che vennero causati dall'introduzione delle navi o degli aeroplani…". E se lo dice lui…
Le applicazioni più probabili di questo Digital Signal Processor saranno infatti nel settore della difesa (crittografia, elaborazione dei dati grafici provenienti da sistemi satellitari, riconoscimento automatico di forme, eccetera) e nell'ambiente multimediale e della comunicazione. E potete già immaginarvi cosa accadrà alla TV: la trasmissione di immagini video ad alta risoluzione a compressioni fantastiche vi porterà in casa una impressionante scelta di canali. Ma c'è chi sta già cercando di applicare il processore ottico alle nuove consolle, per giocare a velocità mai viste …



## IL GRANDE FRATELLO PASSA PER LE MUTANDE

Radio Frequency IDentification: passa da questa sigla la morte dei codici a barre e la nascita dello spyware nelle mutande. C'è gran fermento nelle associazioni dei consumatori americani: prevedono la sostituzione dei codici a barre associati ai barattoli della marmellata e agli altri prodotti da supermercato con etichette 'attive'. In grado, quindi, di inviare dati di prezzo, quantità e tipologia di prodotto direttamente ai ricevitori posti alle casse.
Non solo si avvicina la scomparsa delle cassiere, ma soprattutto si teme che qualche azienda di produzione dei vestiti possa inserire il chip direttamente nel tessuto. Sarebbe così possibile capire quante volte il cliente torna in negozio, o perfino quali e quanti negozi va a visitare. Al di là dei poco ortodossi fini commerciali, significa in sostanza poter tracciare facilmente tutti gli spostamenti di una persona, in sostanza ogni volta che esce da casa.
C'è anche chi sostiene che ad un'etichetta del genere sia possibile associare un numero identificativo unico e personale, valido universalmente. Una sorta di tracciatore che, se occultato, porterebbe veramente alla scomparsa del gioco di nascondino.
Peraltro molte ricerche di mercato non danno RFID come uno standard facilmente utilizzabile, ma in Europa la catena di grande distribuzione Metro è in fase di avanzata sperimentazione delle etichette RFID, così come Wal-Mart e Marks&Spencer negli Stati Uniti.
Tutti concordano, peraltro, che sarebbe prima necessaria una legislazione adeguata, che porti a dei limiti di utilizzo dei chip RFID se questi intaccano la privacy delle persone 'normali'. Ma si sa: fatta la legge, e con la tecnologia giusta...




**Maxell ha sviluppato un chip RFID notevolmente piccolo, piazzando l'antenna direttamente sulla superficie del chip. Robustezza, affidabilità e... occultamento sono garantiti.**





# Te lo do io il Beta-Brite

## Un vecchio Apple IIgs e un po' di sano hacking come lo si faceva una volta permettono di programmare in modo ingegnoso un display a scorrimento

**Il suo nome è Dave Lyons e la sua pagina Web è http://www.lyons42.com. Dave ha ancora un Apple IIgs**, macchina che è andata fuori produzione oltre dieci anni fa e, nelle sue parole, "ha come unico scopo nella vita stare sopra il mio entertainment center e comunicare con vari apparecchi", tra cui un commutataore audio/video fatto in casa di nome Patchboy, un caller ID che mostra il numero di chi chiama a casa Lyons e un display a scorrimento come quelli che si vedono nei negozi, marca Beta-Brite (http://www.betabrite.com). L'Apple IIgs fa da anello di congiunzione tra gli apparecchi e fa in modo che il Beta-Brite mostri, per default, l'ora del giorno, e quando arriva una chiamata mostri il numero del chiamante. Se arrivano più telefonate, mostra anche il numero di chiamate arrivate. Durante gli squilli di una chiamata il Beta-Brite fa scorrere sullo schermo il numero telefonico, l'identità del chiamante (se è nota) e persino lo stato americano da cui proviene la chiamata. Quest'ultima informazione è codificata nel programma scritto in AppleSoft Basic che coordina il tutto e che potete trovare sul sito di Hacker Journal (qui ne viene riportato un frammento in una figura).

Sul sito di Dave si possono trovare tutte le informazioni su come sono interfacciati i vari componenti nonché un altro po' di foto. Se c'è qualcuno tra i nostri hacker che ha combinato qualcosa di simile, ci scriva e sarà ospitato molto volentieri in questa pagina!

**Barg the Gnoll**
**gnoll@hackerjournal.it**

```
21900 REM * message T$
21910 M$ = "A"
22000 REM * text t$
22005 GOSUB 22500
22010 CMD$ = "A" + M$ + T$
22020 GOSUB 24000
22025 T0 = 0: REM reset timer
22030 RETURN
22040 :
22500 REM * translate special characters in T$
22510 T0$ = T$:T$ = ""
22520 IF T0$ = "" THEN 22590
22530 CH$ = LEFT$ (T0$,1):T0$ = MID$ (T0$,2)
22535 IF CH$ = "<" THEN GOSUB 22700: GOTO 22580
22540 IF CH$ < > "$" THEN 22580
22550 CH$ = LEFT$ (T0$,1):T0$ = MID$ (T0$,2)
22555 IF CH$ = "$" THEN 22580
22560 GOSUB 22600:V = DEC:CH$ = LEFT$ (T0$,1):T0$ = MID$ (T0$,2): GOSUB
22600:V = V * 16 + DEC:CH$ = CHR$ (V)
22580 T$ = T$ + CH$: GOTO 22520
22590 RETURN
22595 :
22600 REM * return dec = value of CH$
22610 IF CH$ > = "0" AND CH$ < = "9" THEN DEC = ASC (CH$) - 48: RETURN
22620 IF CH$ > = "a" THEN CH$ = CHR$ ( ASC (CH$) - 32)
22630 IF CH$ > = "A" AND CH$ < = "F" THEN DEC = ASC (CH$) - 55: RETURN
22640 DEC = 0: RETURN
22690 :
22700 REM * Parse a "<...>" string
22710 CH$ = LEFT$ (T0$,1):T0$ = MID$ (T0$,2)
22720 IF CH$ = "<" THEN RETURN : REM * "<<" makes a "<"
22730 TK$ = ""
22740 IF CH$ = ">" OR T0$ = "" THEN 22760
22745 IF CH$ < = "Z" AND CH$ > = "A" THEN CH$ = CHR$ ( ASC (CH$) + 32)
22747 TK$ = TK$ + CH$
22750 CH$ = LEFT$ (T0$,1):T0$ = MID$ (T0$,2)
22755 GOTO 22740
22760 CH$ = ""
22770 IF TK$ = "hold" THEN CH$ = CHR$ (27) + " b"
22771 IF TK$ = "time" THEN CH$ = CHR$ (19)
22780 IF TK$ = "red" THEN CH$ = CHR$ (28) + "1"
22781 IF TK$ = "green" THEN CH$ = CHR$ (28) + "2"
22782 IF TK$ = "amber" THEN CH$ = CHR$ (28) + "3"
22783 IF TK$ = "lred" THEN CH$ = CHR$ (28) + "4"
22784 IF TK$ = "lgreen" THEN CH$ = CHR$ (28) + "5"
22785 IF TK$ = "brown" THEN CH$ = CHR$ (28) + "6"
22786 IF TK$ = "orange" THEN CH$ = CHR$ (28) + "7"
22787 IF TK$ = "yellow" THEN CH$ = CHR$ (28) + "8"
22788 IF TK$ = "rb1" THEN CH$ = CHR$ (28) + "9"
22789 IF TK$ = "rb2" THEN CH$ = CHR$ (28) + "A"
22790 IF TK$ = "mix" THEN CH$ = CHR$ (28) + "B"
22800 IF TK$ = "cr" THEN CH$ = CHR$ (27) + " t": RETURN
22801 IF TK$ = "rotate" OR TK$ = "rot" THEN CH$ = CHR$ (27) + " a": RETURN
22810 IF TK$ = "welcome" THEN CH$ = CHR$ (27) + "0n8"
22811 IF TK$ = "nosmoke" THEN CH$ = CHR$ (27) + "0nU"
22812 IF TK$ = "special" THEN CH$ = CHR$ (27) + "0n"
22813 IF TK$ = "horse" THEN CH$ = CHR$ (27) + "0nW"
22814 IF TK$ = "thanks" THEN CH$ = CHR$ (27) + "0nS"
22990 RETURN
22995 :
23000 REM * Set up a handy memory configuration
23010 CMD$ = "E$AAU0800FF00BAU0800FF00"
23020 GOSUB 24000
23090 RETURN
23095 :
24000 REM  * send cmd$, no response
24010 PRINT D$;"PR#1"
24020 PRINT NUL$; CHR$ (1);"Z00"; CHR$ (2);CMD$; CHR$ (4)
24025 PRINT D$;"PR#0"
24030 RETURN
24999 :
25000 REM * Initialize
25005 TRUE = (1 < 2):FALSE = NOT TRUE
25010 D$ = CHR$ (4)
25610 NUL$ = CHR$ (0) + CHR$ (0) + CHR$ (0) + CHR$ (0) + CHR$ (0) + CHR$
(0) + CHR$ (0) + CHR$ (0) + CHR$ (0) + CHR$ (0)
25620 RETURN
25630 :
25900 REM * INIT SCREEN
25910 TEXT : HOME : NORMAL : SPEED= 255: NOTRACE
25922 PRINT HH$;"BetaBrite v";VN$;" ";DT$;HH$
25930 POKE 34,4
25935 HOME
25940 RETURN
25990 :
30000 REM * CallerID INIT
30005 REM * Data at $360 for slot 2 status/read
30010 DATA 162,194,160,32,169,1,32,72,194,169,0,42,133,0,96,234,162,194,160,32,32,70,194,133,0,96
30020 FOR A = 864 TO 889: READ B: POKE A,B: NEXT
30030 PRINT CHR$ (4);"PR#2": PRINT : PRINT CHR$ (4);"PR#0"
30050 DIM CID$(50):NC = 0
30090 RETURN
30099 :
30900 REM * "#" simulate incoming call
30910 VTAB 24: HTAB 1: PRINT : PRINT
30920 INPUT "CID$: ";CID$
30925 IF CID$ = "" THEN RETURN
30926 IF LEN (CID$) = 3 THEN CID$ = CID$ + "0000000"
30927 IF CID$ = "2" THEN CID$ = "4082539779"
30930 CID$ = "xxxxxxxx" + CID$
30950 GOSUB 31145
30960 RETURN
30970 :
31000 REM * Incoming CallerID character
31010 CALL 880
31020 IF PEEK (0) = 4 THEN 31100
31030 IF PEEK (0) = 128 THEN 31500
31090 RETURN
31095 :
31100 REM * SMDF format (just a phone number)
31110 CALL 880:L = PEEK (0)
31115 CID$ = ""
31120 FOR I = 1 TO L: CALL 880:CID$ = CID$ + CHR$ ( PEEK (0)): NEXT
31130 CALL 880:CK = PEEK (0)
31140 CALL 864: IF PEEK (0) THEN CALL 880: GOTO 31140
31145 REM * CID$ = "mmddhhmm#..."
31147 NC% = NC% + 1
31150 NN$ = MID$ (CID$,9)
31175 GOSUB 32000
31200 T$ = "<hold>": IF LEN (NN$) > 14 THEN T$ = "<cr>"
31205 T$ = T$ + "<green>" + NN$: GOSUB 21900
31210 T0 = 500: REM countdown till retoring display
31250 GOSUB 33500: REM Log
31300 RETURN
31310 :
31500 REM * MDMF format (multiple messages)
31505 C1$ = "":C2$ = "":C3$ = "": REM c1$=time, c2$=number, c3$=name
31510 CALL 880:L9 = PEEK (0)
31515 REM * next param in msg
31520 CALL 880:T = PEEK (0)
31530 CALL 880:L = PEEK (0)
31540 C$ = "": FOR I = 1 TO L: CALL 880:C$ = C$ + CHR$ ( PEEK (0)): NEXT
31550 IF T = 1 THEN C1$ = C$: GOTO 31600
31560 IF T = 2 OR T = 4 THEN C2$ = C$: GOTO 31600
31570 IF T = 7 THEN C3$ = C$
31600 REM * get get param, if any
31610 L9 = L9 - L - 2: IF L9 > 0 THEN 31515
31700 IF C3$ = "" THEN CID$ = C1$ + C2$: GOTO 31140: REM * fall through to old code
31710 NN$ = C2$: IF LEN (NN$) = 10 THEN NN$ = LEFT$ (NN$,3) + " " + MID$ (NN$,4,3) + "-" + MID$ (NN$,7)
31712 IF LEN (NN$) = 1 THEN GOSUB 32000: REM O and P
31715 LL$ = ""
31720 IF LEFT$ (NN$,4) = "408 " THEN NN$ = MID$ (NN$,5): GOTO 31800
31750 AA% = VAL ( LEFT$ (NN$,3)): GOSUB 34000
31800 REM * NN$ = number, C3$=name, LL$=area code
31810 T$ = "<hold><cr><green>" + NN$
31820 IF C3$ < > "" THEN T$ = T$ + "<red> " + C3$
31830 T$ = T$ + "<orange> " + LL$
31850 GOSUB 21900: REM * msg T$
31860 T0 = 750: REM countdown till restoring display
31900 CID$ = C1$ + NN$ + " " + C3$ + LL$: GOSUB 33500
31910 RETURN
31990 STOP
31995 :
32000 REM * Translate well-known phone numbers (NN$)
32002 IF NN$ = "O" THEN NN$ = "Out of area": RETURN
32003 IF NN$ = "P" THEN NN$ = "Private call": RETURN
32005 IF LEN (NN$) = 10 THEN NN$ = LEFT$ (NN$,3) + " " + MID$ (NN$,4,3) + "-" + MID$ (NN$,7)
32007 C9$ = " <orange>"
...
32070 IF NN$ = "408 257-5555" THEN NN$ = NN$ + C9$ + " Pizza Presto": GOTO 32900
...
32800 IF LEFT$ (NN$,7) = "408 253" THEN NN$ = NN$ + C9$ + "probably Apple": RETURN
32900 :
32960 IF LEFT$ (NN$,4) = "408 " THEN NN$ = MID$ (NN$,5): RETURN
32970 AA% = VAL ( LEFT$ (NN$,3)): GOSUB 34000: IF LL$ < > "" THEN NN$ = NN$ + " <orange>" + LL$
32990 RETURN
32995 :
33000 REM * Review CallerID calls
33010 TEXT : HOME : PRINT HH$;"Review recent calls": PRINT HH$: POKE 34,3
33020 PRINT "Number of calls: ";NC
33030 IF NC = 0 THEN 33210
33040 FOR I = 1 TO NC
33050 CID$ = CID$(I)
33060 PRINT LEFT$ (CID$,2);"/"; MID$ (CID$,3,2);" ";
33070 PRINT MID$ (CID$,5,2);":"; MID$ (CID$,7,2);" ";
33080 NN$ = MID$ (CID$,9)
33090 IF NN$ = "O" THEN NN$ = "Out of area"
33100 IF NN$ = "P" THEN NN$ = "Private call"
33110 N0$ = NN$: GOSUB 32000
33120 PRINT N0$;: IF NN$ < > N0$ THEN PRINT " (";NN$;")";
33130 PRINT
33200 NEXT
33210 GET A$: RETURN
33220 :
33500 REM * Log CID$
33510 NC = NC + 1
33520 IF NC = 50 THEN FOR I = 1 TO 40:CID$(I) = CID$(I + 10): NEXT : FOR I = 40 TO 49:CID$(I) = "": NEXT :NC = 40
33528 ZZ$ = CID$:CID$ = "": FOR I = 1 TO LEN (ZZ$):CC = ASC ( MID$ (ZZ$ + " ",I,1)): IF CC < 32 OR CC > 127 THEN CC = 32
33529 CID$ = CID$ + CHR$ (CC): NEXT
33530 CID$(NC) = CID$
33540 REM * flush any garbage characters from incoming serial
33550 FOR I = 1 TO 9000: NEXT
33560 CALL 864: IF PEEK (0) THEN CALL 880: GOTO 33560
33570 RETURN
33990 :
33999 :
34000 REM * Compute LL$ = descr of area code AA%
34010 LL$ = AA$(AA%(AA%)): RETURN
34199 :
34200 REM * Init area code data
34205 DIM AA%(1000),AA$(100)
34210 FOR I = 1 TO 1000
34220 READ AA$(I): IF AA$(I) = "*" THEN RETURN
34230 FOR J = 1 TO 2 STEP 0: READ A: IF A = 0 THEN 34240
34235 IF AA%(A) THEN STOP
34237 AA%(A) = I: NEXT
34240 NEXT I: STOP
34295 :
34300 REM * Area code data
34500 DATA Alberta,403,780,0
34505 DATA Alabama,205,256,334,0
34510 DATA Alaska,907,0
34515 DATA Arizona,520,602,0
34516 DATA Arkansas,501,0
34520 DATA Bahamas,242,0
34521 DATA Barbados,246,0
34525 DATA Bermuda,441,0
```

# CRACCARE SKY la sfida è aperta

**Sono davvero finiti i giorni della cuccagna per chi piratava la tv a pagamento? La codifica di Sky sembra inattaccabile, ma prima di dire l'ultima parola...**

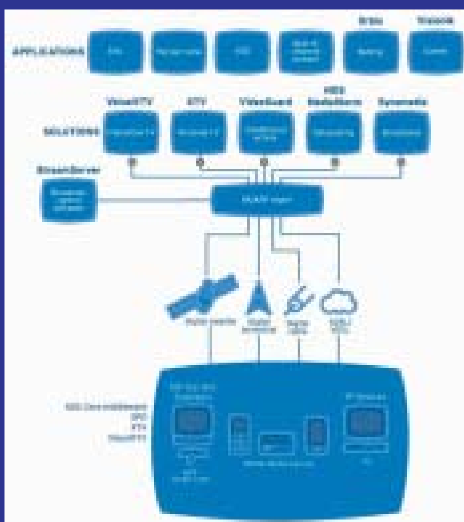
**Sembrava diventato lo sport nazionale, procurarsi la scheda pirata per guardare a sbafo la pay-per-view.** Alla goduria di vedersi la partita si sommava il gusto di invitare gli amici a vederla, passando per furbacchioni: io sì che so vivere, ragazzi, vedo persino gratis le partite e i film di quasi prima visione.

Poi è arrivatoil Seca2 prima, e Sir Rupert Murdoch con Sky Tv poi, e la musica è cambiata, e di brutto anche. Tutto un mercato di contraffattori e faccendieri sembra essersi esaurito di botto. Nei salotti girano facce moge e qualcuno, disperato, ha addirittura messo mano al portafogli e si è rifatto il bouquet (che a dirla così pare si risposi, e invece si è abbonato a Sky).
Ora, d'accordo sul fatto che rubare i programmi della tv a pagamento è disonesto; ma il vero hacker, senza la minima intenzione di rubare alcunché, vorrà comunque sviscerare il sistema di Sky e scoprire se vi sono punti deboli, magari per segnalarli a Sky stessa. Siamo interessati a come funzionano le cose, non a rubarle, giusto?
**Giusto. E allora vediamo un po' come stanno le cose con Sky Tv e i suoi sistemi di codifica.**

## >> In principio era Irdeto

Il segnale della vecchia Stream era codificato con il sistema Irdeto prima versione, che è stato craccato con relativa facilità. Il segnale attuale di Sky, invece, utilizza le tecnologie Irdeto2, Seca2 e NDS. Irdeto2 risulta non craccato. Seca2 pare sia stata craccato, invece. Nell'ambiente si sussurra di gente a caccia di "bianchine" e card originali scadute, che sarebbe possibile riattivare a patto di disporre dei log di attivazione e che questi risalgano a prima di una certa data. Per questo sembra che Sky ormai stia vendendo solo abbonamenti basati su tecnologia NDS. In ogni caso non sarebbero procedure replicabili a casa propria, ma richiederebbero capacità industriali. Inoltre basterebbe che Sky organizzasse un rinnovo delle card agli abbonati per vanificare un pirataggio eventualmente riuscito. Senza contare che le chiavi cambiano con frequenza molto maggiore, anche più volte al giorno, rispetto ai sistemi precedenti, e questo complica notevolmente la vita ai pirati: chi può permettersi di aggiornare la propria card piratata magari due volte al giorno?



NDS fa ben più che fabbricare i sistemi di codifica di Sky.

Per capire ancora meglio la forza di Seca2 rispetto al suo predecessore Seca1, bisogna pensare che con Seca2 i comandi gestiti dal sistema operativo della scheda vengono cifrati con chiavi presenti in una parte inaccessibile della scheda stessa. A confronto, il sistema operativo delle card Seca1 presentava alcuni bug che consentivano di ottenere in chiaro le chiavi di gestione, a patto di impartire comandi contenenti byte specifici posizionati in punti strategici del comando stesso. Una volta ottenute le



Ministero dell'Interno

DIPARTIMENTO DELLA PUBBLICA SICUREZZA

Direzione Centrale per la Polizia Stradale, Ferroviaria, di Frontiera e Postale

Servizio di Polizia Postale e delle Comunicazioni

AREA INTERNET

http://www.digitalsin.org

SOTTOPOSTA A SEQUESTRO

DECRETO NR. 34179/01 DELLA PROCURA DELLA REPUBBLICA

PRESSO IL TRIBUNALE DI ROMA

La pirateria tv tempo fa aveva vita assai più facile.

chiavi di gestione, non era difficile decrittare le chiavi operative mensili che aprivano la via alla visione, per esempio, della vecchia Tele+. C'era modo sotto Seca1 anche di ottenere la master key, la chiave legata alla card specifica, mentre per ora non pare esistano metodi rapidi per fare la stessa cosa con Seca2.

Gli algoritmi di cifratura di Seca2 sono abbastanza noti, solo che le chiavi hanno una lunghezza (da otto a sedici byte) tale che un attacco brute force richiederebbe un numero di anni spaventosamente alto (pensate a 10 seguito da quindici-venti zeri) per avere una buona probabilità di farcela solamente a suon di calcolo.

Anche per quanto riguarda il sistema NDS (http://www.nds.com) uno dei punti di forza antipirateria è che viene stabilita una precisa corrispondenza tra ciascuna card da inserire nel decoder e ciascun decoder. Insomma per superare le protezioni di Sky non basta emulare una card qualsiasi, ma occorre ricostruire il gemellaggio tra un decoder specifico e la "sua" card. O riuscire a riprogrammare un decoder in modo che accetti più di una card.



La sfida al sistema di cifratura di Sky è stata lanciata da tempo. Chi la vincerà?

Per il momento, in definitiva, si fa un gran parlare di alternative ma la verità è una: a parte mio cuggino (avete presente Elio e le Storie Tese? "Mi ha detto mio cuggino che da bambino una volta è morto…"), il sistema di cifratura adottato da Sky per le sue trasmissioni è a prova di cracker o, almeno, di cracker artigianale.

Immagino che i progressi più sensibili avverranno dove è possibile lavorare interamente o quasi via software, ossia in emulazione. Per chi ha un impianto satellitare con scheda di ricezione dentro un PC esistono programmi come Multidec (http://www.multidec-italia.da.ru) che emulano un decoder e relativa card. Per ora con NDS non ce l'hanno fatta neanche loro. Ma forse è solo questione di tempo. Va da sé che anche qui ci si sta studiando sopra e che sul sito di Hacker Journal potremmo fare un bel lavoro di scambio di idee. Per saperne di più naturalmente, e non per piratare. O c'erano dubbi?

**Kurt Gödel**
**kurtgoedel@hackerjournal.it**

# TIPS

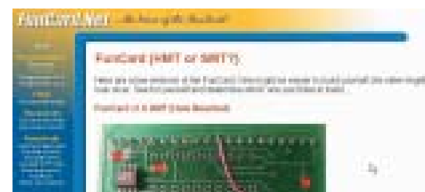
## IL TRUFFATORE TRUFFATO

Chiamiamolo Gigetto. Gigetto è un furbetto, sempre a caccia del chip per modificare la PlayStation, del DVD craccato e naturalmente anche della tv a sbafo. Gigetto un giorno ha parlato con l'amico di un amico di un amico che gli ha detto "te lo allargo io l'abbonamento!" (pronunciare con accento bolognese, se guardate Zelig), ossia, ti faccio vedere più di quello che hai pagato. Il tizio ha chiesto tutti i dati di utenza a Gigetto e, per una modica somma, gli ha davvero allargato l'abbonamento: usando i dati di Gigetto, ha comprato a suo nome tutto il comprabile, si è tenuto la modica cifra e tanti saluti. Gigetto, il mese dopo, si è visto sulla carta di credito un conto da paura.

Per ogni Gigetto c'è sempre qualcuno più furbo di lui…

## IN DUE PAROLE

Funcard: card programmabile, anche fatta in casa. http://www.funcard.net.
MOSC: Modifiked Original Smart Card.



**Domanda:** In generale le protezioni del software sui computer durano molto poco. Perché le protezioni della tv a pagamento sono così ostiche?

**Risposta:** La combinazione software più hardware crea molte più difficoltà al pirata di una protezione solo sw. Inoltre è una questione di finestre di utilizzo: craccare un sw significa magari poterlo utilizzare per mesi o anni. Se lo sforzo di craccare un sistema di card più decoder richiede tempo e fatica ma è vanificabile nel giro di pochi giorni, diventa molto meno appetibile. Poi non tutti dispongono della tecnologia e delle conoscenze richieste. Infine, sui moderni sistemi di protezione delle trasmissioni tv è possibile che le chiavi da identificare cambino anche più volte al giorno. Sono tutte cose che, nel campo del puro sw, non esistono.

# TERRORISMO & CIBERNETICA

**I terroristi usano la tecnologia per non farsi beccare, le forze dell'ordine per beccare i terroristi. A chi il prossimo round?**

È recente la notizia dell'arresto di una decina di presunti brigatisti rossi (alcuni dei quali peraltro si sono già dichiarati prigionieri politici) che, secondo le forze dell'ordine, avrebbe assestato un colpo mortale alle Brigate Rosse in via di riorganizzazione.
Subito una premessa: non è che le forze dell'ordine mi stiano particolarmente simpatiche. Però, tra terroristi che colpiscono per uccidere persone comuni e poliziotti che cercano di fermarli, io voto poliziotti, tutta la vita.
Detto ciò, in questo articolo riassumiamo alcune delle tappe più recenti della guerra tra guardie e ladri, buoni e cattivi, volendo virus e antivirus, guardando alle tecnologie usate e a come sono state recentemente usate… o abusate.

## >> PGP è davvero sicuro?

Fatta la premessa, andiamo al succo: l'ondata di arresti è frutto del fermo di Nadia Desdemona Lioce, seguito a uno scontro a fuoco su un treno in cui hanno perso la vita il terrorista Mario Galesi e l'agente Polfer Emanuele Petri. Galesi e Lioce avevano con sé alcune borsone contenenti, tra l'altro, un "palmare" Psion 5MX. Non è esattamente un palmare quanto un computer portatile, con una tastiera piccola ma utilizzabile in ogni momento. Una terrorista ha forti requisiti di mobilità e di sicurezza. I suoi dati devono essere tutti con sé, pena correre gravi rischi. E infatti la polizia trova dentro il palmare ben 106 file, dalle deliranti "risoluzioni strategiche" a – ben più importante – nomi, agende, numeri di telefono. Lioce e Galesi conoscevano l'esistenza di PGP, di cui esiste una versione per il sistema operativo Epoc dei computer Psion, e lo avevano usato per cifrare alcuni loro documenti. Qui le versioni divergono: alcuni sostengono che la polizia sia riuscita a leggere una serie di dati dalla memoria tampone del computer, la zona temporanea in cui risiedono i dati in elaborazione prima di essere salvati (e cifrati); altri sostengono che è stato possibile violare la cifratura di PGP grazie all'aiuto dell'FBI. Allora PGP non è sicuro e ci fanno credere il contrario? Secondo me i dati cifrati di Nadia Lioce sono ancora tali. A meno che non siano state usate una cifratura relativamente debole e una password banale. PGP è sicuro solo perché ci vuole moltissimo tempo a calcolare la chiave di cifratura avendo a disposizione solo la chiave pubblica e il testo cifrato. Decifrare



Tradita dalla memoria. Del suo computer da tasca.

un messaggio PGP su ciascun computer del mondo è un compito impossibile, oggi. Concentrarsi su un singolo computer è diverso. E se, come sembra, la password di posta elettronica della brigatista era "Aristide", quella usata in PGP non sarà stata meglio. Il 99,9 per cento dei lettori di Hacker Journal è capace di escogitare una password migliore.

## >> Osama sim Laden

Dal carcere Lioce e compagni hanno fatto l'apologia di Osama bin Laden e della rete terroristica di Al Qaeda. Dello sceicco è nota l'abitudine alla steganografia, ossia a nascondere messaggi all'interno di file grafici o sonori, distribuendo i byte del messaggio sotto forma di quasi indistinguibili imperfezioni del file (solitamente file porno o MP3,

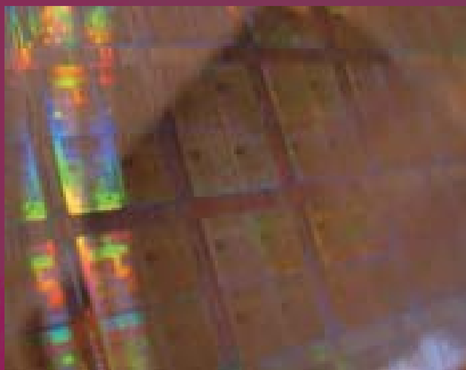


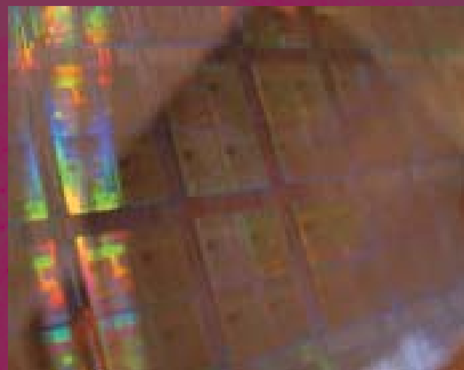

o altri tipi di file molto diffusi in Rete). Esistono programmi che vanno a caccia, con vario successo, di messaggi steganografici; cosa leggermente meno nota è che la steganografia può passare anche attraverso la comune posta elettronica. Un sistema semplice ma ingegnoso detto snow consiste nel distribuire alla fine di ciascuna riga di messaggio un certo numero di spazi bianchi. Dal loro numero e dalla loro disposizione è possibile risalire al messaggio autentico.
Il governo americano le sta provando tutte e non ha esitato a spendere somme ingenti nella simulazione software. Il Modeling, Virtual Environments and Simulation Institute (http://movesinstitute.org) di Monterey, nelle vicinanze di San Francisco in Califor-

nia, avrebbe trenta ingegneri al lavoro su molti progetti tra cui uno denominato, ironicamente, Osama sim Laden. Il progetto mirerebbe a ricostruire nella simulazione le città e le infrastrutture americane per vedere quanto e come possono essere vulnerabili ad attacchi terroristici e, all'opposto, intende riprodurre scenari in cui unità militari relativamente ridotte in numero devono contrastare azioni di guerra non convenzionale condotte da guerriglieri o piccoli gruppi di attentatori.
Viene facile la battuta: speriamo che almeno nelle simulazioni siano capaci di prendere Osama! D'altro canto da questi progetti derivano anche prodotti quanto meno singolari, come il videogame America's Army, prodotto direttamente dall'esercito degli Stati Uniti.

## >> Vuota le tasche

La prossima edizione del Super Bowl americano sarà la seconda in cui agli ingressi saranno impiegati i face detector. Questi dispositivi sono composti da telecamere digitali collegate a computer molto potenti.





**Queste immagini non sono identiche (è un wafer di silicio pieno di processori), ma in una è stata nascosta, mediante steganografia, la frase "La steganografia è un mezzo eccellente per nascondere testo all'interno delle immagini." Riuscite a cogliere la differenza? Scommetto di no.**

Le telecamere inquadrano fino a quindici visi al secondo e i computer, in tempo reale, stabiliscono se i volti corrispondono a quelli di persone ricercate. Non è un sistema dalla sicurezza assoluta ma permette di rafforzare notevolmente i controlli in modo relativamente indolore in situazioni come gli ingressi (aree circoscritte e note) di uno stadio. Relativamente indolore, perché c'è un buon numero di falsi positivi e conseguentemente di spettatori che vengono fermati e controllati pur non essendo affatto ricercati, ma solo somiglianti, per il computer, a facce note.
Altre tecnologie che vedremo nei prossimi anni in aeroporti e stazioni sono i backscatter, dispositivi decisamente superiori ai tradizionali scanner ai raggi X, così precisi nel visualizzare gli oggetti presenti addosso a una persona da rischiare l'oltraggio al pudore. La californiana Ancore invece produce i Pulsed Fast Neutron Analyzer, scanner giganteschi che esaminano fino all'ultimo spillo il carico di container e autotreni, senza svuotarli o toccarne il contenuto. La Cepheid, fino a poco tempo fa fornitrice esclusiva del Pentagono, è al lavoro nel costruire rilevatori di agenti patogeni (per esempio il virus del vaiolo) sempre più miniaturizzati e veloci nell'individuazione. Lo scopo naturalmente è disseminarli per aeroporti e ogni altro luogo a rischio.

## >> In concreto

Come sempre la tecnologia è neutra: su può usare bene o male, per uccidere o per salvare vite. A noi sulla frontiera dell'hacking, curiosi per natura di come funzionano le cose, va il dovere di vigilare sul corretto impiego delle tecnologie di sorveglianza e di occultamento dei dati. Perché la sicurezza nazionale e collettiva deve andare di pari passo con la privacy individuale.

**Kurt Gödel**
**kurtgoedel@hackerjournal.it**

### Per approfondire

Sulla steganografia: http://www.wowarea.com/italiano/aiuto/stegait.htm
Su America's Army: http://www.americasarmy.com
Sui dispositivi backscatter: http://www.americasarmy.com/
Sugli apparecchi antiagenti patogeni: http://www.cepheid.com/
Sugli scanner a uso industriale: http://www.ancore.com

# TIPS

## LA REPUBBLICA DEGLI ASINI

Secondo Repubblica online i contenuti dello Psion 5 di Nadia Lioce non riuscirebbe a leggerli neanche l'FBI (http://www.repubblica.it/online/cronaca/lioce/fbi/fbi.html) dal momento che "non hanno mai ottenuto dalla Psion, l'azienda americana produttrice di palmari, gli algoritmi su cui si basano i codici sorgenti, cioè le chiavi per decrittare il programma". Forse non si sono accorti che per avere i sorgenti di PGP basta scaricarli da http://www.pgpi.org e che PGP è disponibile in versione totalmente open source. Voto: asini.




## LINUX E LO PSION

Lo Psion 5MX che conteneva i segreti della brigatista Lioce.
Ci gira sopra anche Linux!
Per conferma, consultare
http://sourceforge.net/projects/linux-7110
e
http://staff.washington.edu/dushaw/psion






# Nella TUA comanda

## Bill Gates può fare quello che vuole sulla console che tu h

**I 90 percento dei computer in funzione sulla faccia della Terra si basa su software creato da Microsoft, il colosso creato negli anni Ottanta da Bill Gates.**

Non è che il software Microsoft abbia mai brillato per qualità. Ma non è l'efficienza del sistema operativo più diffuso del mondo a preoccupare, quanto le cose che accadono a utenti Microsoft come Michael Steil.

Michael è un cittadino tedesco sostenitore del software libero. Microsoft vede il software libero come fumo negli occhi (lo ha chiamato recentemente "cancro della proprietà intellettuale") perché sempre più spesso istituzioni e grandi aziende lo preferiscono al software Microsoft, che è chiuso (nessuno può vederlo, a parte alcune eccezioni) e proprietario (nessun può modificarlo).

Seguendo le istruzioni visibili sul sito del progetto Xbox-Linux (http://xbox-linux.sourceforge.net), Michael Steil ha installato Linux sulla sua Xbox, che viene venduta da Microsoft come console per videogiochi ma di fatto è un computer economico. Con Linux funziona a meraviglia e non c'è nemmeno bisogno, come si faceva all'inizio, di "moddarla" con un chip di modifica hardware.

## >> Aggiornamento a sorpresa

Un giorno, mentre Michael gioca a MechAssault, il software aggiorna la Xbox e installa il software di collegamento a Xbox Live, il servizio di gioco online offerto da Microsoft. Ma Michael non si iscrive al servizio e quindi non sottoscrive abbonamenti né contratti di alcun genere né, peraltro, ha richiesto l'aggiornamento software. Sta di fatto che il menu standard della sua Xbox si arricchisce di un nuovo termine, Xbox Live.

Per curiosità Michael seleziona il nuovo comando. XBox gli chiede i parametri di connessione a Internet e si collega, tanto che Michael può vederla in Rete tramite comandi di ping da un altro computer. Però non si iscrive ad alcun servizio di Xbox Live e non accetta alcun contratto di alcun tipo; ha solo inserito i parametri di connessione a Internet per la sua console.

Un altro giorno Michael seleziona nuovamente, per errore, il comando Xbox Live. Immediatamente appare il messaggio

```
Xbox Live is updating your
system. Please don't turn off
your Xbox console.
```

Michael non ha potuto confermare il suo assenso; l'aggiornamento è partito automaticamente. D'altronde adesso fermarlo potrebbe causare danni e quindi Michael lo lascia proseguire.

Al termine dell'operazione controlla e, sorpresa! L'aggiornamento ha cancellato – non aggiornato o modificato o sostituito: cancellato – alcuni dati che risiedevano nel disco della Xbox. Guarda caso, si trattava di file necessari per utilizzare Linux sulla console oppure di dati personali di Michael!

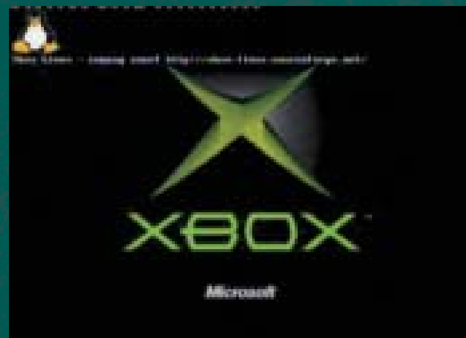
## >> Che succederebbe se Fiat o Sony...?

Le legislazioni dei Paesi europei non sono omogenee, ma sono abbastanza simili e praticamente dappertutto l'episodio sarebbe giudicabile come intrusione indebita in un sistema informatico di proprietà altrui e come tale passibile di sanzioni a vari livelli di gravità.

Immaginate che accaderebbe se una squadra della Fiat passasse di notte a cambiare colore alle Fiat acquistate e parcheggiate in strada, senza permesso




dei proprietari. O se la Sony fulminasse quello che sta appoggiato a casa nostra sopra un suo televisore perché ha deciso che i suoi televisori non vanno usati come soprammobili.




Nel mondo del software quanto è accaduto a Michael Steil non è una novità. Da anni gli acquirenti di Windows accettano implicitamente un accordo, il famigerato EULA (End User License Agreement, accordo di licenza all'utente finale) che usualmente nessuno legge nei

> **"SE NEL NOME C'È UNA X È UNIX. QUINDI LA XBOX DEVE ESSERE UNIX"**
>
> da una discussione su Slashdot.org




# Xbox Microsoft



hai pagato. Anche cancellare la tua installazione di Linux

dettagli. L'EULA stabilisce che chi compra una copia di Windows non ne diventa proprietario, ma acquisisce una sorta di diritto all'utilizzo, che formalmente è soggetto all'arbitrio di Microsoft e può cessare in qualunque istante Microsoft lo voglia. Qui la cattiva non è solo Microsoft; più o meno tutte le aziende di software si comportano in modo simile.

Con l'hardware invece il problema è differente. Fino a oggi il computer è stato un bene materiale, che viene acquistato in via definitiva e di cui l'acquirente dispone a suo piacimento. Ci sono vecchi computer che sono stati trasformati in acquari o jukebox e dovrebbe essere una cosa del tutto normale. Ma quanto accaduto a Michael Steil mette pesantemente in discussione questo quadro.




## E domani Palladium

Forse è solo un esempio di quello che sta per arrivare. Microsoft ha già ricevuto critiche severe in passato per i suoi progetti della cosiddetta gestione digitale dei diritti d'autore, o DRM (Digital Rights Management), altrimenti denominata Palladium. Svelato dalla stampa specializzata in anticipo sui progetti dell'azienda, Palladium si è rivelato un sistema sì di gestione, ma anche della libertà dell'utente, che in linea di principio – su un computer dotato di DRM – può compiere solo azioni che il sistema considera come legittime, al punto che il lettore dei CD-ROM può bloccarsi se non è previsto che l'utente decida, per esempio, di ricavare file audio MP3 a partire dai brani presenti sul CD stesso.

Microsoft ha messo l'accento sugli aspetti positivi di Palladium (per esempio aumenta grandemente la sicurezza dei sistemi), ma rimane il fatto che, un domani non lontano, potremmo non essere più pienamente padroni di quello che acquistiamo.

Michael Steil potrebbe non essere un utente particolarmente sfortunato di Xbox, ma un pioniere nella denuncia della violazione di diritti che, in assenza di vigilanza, rischiamo di dover dimenticare.

**Reed Wright**
**reedwright@mail.inet.it**



### link

http://xbox-linux.sourceforge.net/
Per scoprire tutto sul progetto Xbox-Linux.

http://xbox-linux.sourceforge.net/docs/remotedelete.html
Per leggere la storia dettagliata di come Microsoft ha cancellato a Michael i file di Linux e personali residenti sulla sua Xbox.

http://xbox-linux.sourceforge.net/docs/gettingstarted.html
Per montare Linux sulla tua Xbox!

## TIPS

### CONSOLE, ANZI NO COMPUTER

Queste, in breve, le spcciffiche tecniche di Xbox:

- Processore Intel Celeron a 733 MHz
- Scheda video GeForce 3MX nVidia
- 64 MB of RAM
- Scheda audio Dolby Digital 97
- Disco rigido da 8/10 GB
- Lettore DVD
- Connessione Ethernet 10/100
- 4 porte USB

Come si vede, anche se viene venduta come console, è in realtà un comune computer, con specifiche assai limitate secondo lo standard di oggi.

### ARRIVA POWERPC

Le prossime generazioni di Xbox non conterranno un processore fabbricato da Intel, come i Pentium e i Celeron, ma realizzati da IBM, che ha recentemente annunciato un accordo in questo senso stretto proprio con Microsoft. Il comunicato ufficiale di IBM si può leggere all'indirizzo http://www.ibm.com/news/us/2003/11/031.html.

### LOGO OPENSOURCE




Il logo del CD di Xbox Linux (sopra), scelto dopo un concorso che ha visto decine di proposte da tanti appassionati. A http://xbox-linux.sourceforge.net/docs/cdart.html si possono vedere tutte le alternative.








# P2P: parla il BOSS di

**Una bambina di dodici anni, gli attacchi delle major, nuovi sviluppi della tecnologia:**

**Quanto segue è un libero ma fedele estratto di un'intervista concessa a OpenP2P.com da Greg Bildson, Chief Operating Officer di LimeWire e President di P2P United, un consorzio di aziende del peer-to-peer creato per spiegare meglio ai politici e al pubblico il valore delle tecnologie e della cultura peer-to-peer.** Il testo originale dell'intervista si può leggere a http://www.openp2p.com/pub/a/p2p/2003/11/14/limewire.html.

**Brianna LaHara**, newyorchese di Manhattan dai capelli ricci, ha dodici anni ma ha già fatto in tempo a sporcarsi la fedina penale: ha usato un software peer-to-peer, come Xnap, WinMX o LimeWire. Per la precisione ha usato Kazaa ed è stata denunciata dalla RIAA (Recording Industry Association of America) per avere scaricato musica "illegalmente". Le parti si sono accordate per una multa di duemila dollari (poco meno di 1.700 euro) ma la RIAA ha rivendicato per sé la possibilità di richiedere risarcimenti anche di 150 mila dollari a canzone "piratata". Insieme a Brianna sono rimaste coinvolte nell'azione penale altre 260 persone, ma per la dodicenne, dopo che erano già state aperte diverse collette su Internet, ha pagato la sanzione P2P United (http://www.p2punited.org), organizzazione che vede Greg Bildson tra i fondatori.

---

**D.: Allora avete pagato la multa di Brianna?**

**R.**: *Sì, abbiamo rimborsato sua madre. Sentivamo che citare in giudizio una dodicenne non era una risposta.*




**"I detentori di copyright non dovrebbero essere in grado di danneggiare i progressi della tecnologia allo scopo di proteggere i loro vecchi modelli di business".**

**D.: Possiamo sapere qualcosa di più su P2P united?**

**R.**: *P2P United sta provando a evitare che il Congresso degli Stati Uniti faccia qualcosa di stupido nel campo tecnologico, di cui sanno poco. Subiscono la cattiva propaganda della RIAA e dobbiamo fare qualcosa, specialmente quando si accampano scuse come pornografia o sicurezza nazionale, che per quanto riguarda il peer-to-peer sono problemi del tutto minori. E comunque, in questi casi, è il contenuto di per sé a essere illegale: il fatto che il contenuto illegale transiti o meno via peer-to-peer non è un problema del peer-to-peer, esattamente come non è un problema delle linee telefoniche se due pedofili si telefonano. Se il governo deve regolamentare qualcosa, è meglio che sappia che cosa sta facendo.*

---

**D.: E così spiegate al Congresso come stanno le cose.**

**R.**: *Non è che al Congresso muoiano dalla voglia di saperlo, ma ci proviamo. Per ora si sono dimostrati intenzionalmente ciechi o ignoranti.*

---

**D.: Pensate che la RIAA alla fine possa scoprire qualche modo in cui il peer-to-peer possa conciliarsi con il loro modello di business?**

**R.**: *Speriamo di sì. L'industria ci vede come nemici ma sono convinto che esistano soluzioni che vedono vincere tutti.*

---

**D.: Che cosa pensi dei nuovi negozi di musica online, come l'iTunes Music Store e Buymusic.com?**

**R.**: *Sono passi nella giusta direzione, ma c'è un sovrapprezzo radicale. Nell'era digitale non ha senso che una canzone costi 99 centesimi di dollari; dovrebbe costarne cinque. Un altro problema è che il Digital Rights Management (DRM) creato da Microsoft appare troppo restrittivo. C'è un trend di siti pay-per-download che usano tutti DRM e mettere in mano a Microsoft un altro monopolio non mi sembra furbo.*

---

**D.: Parlaci di MagnetMix.**

**R.**: *MagnetMix (http://magnetmix.com) è un nuovo esempio di integrazione tra peer-to-peer e Web. Il Web può presentare le cose in modo più gradevole, mentre i programmi P2P possono funzionare come una specie di Google più grez-*





# LIME WIRE

il peer-to-peer come avamposto della libertà di espressione

*zo. In parole povere, l'artista – invece o insieme al proprio sito Web – crea un pacchetto di contenuto multimediali tenuto insieme da pagine HTML, lo comprime in un unico singolo file .zip e mette il file a disposizione sulle reti P2P.*

---



**Brianna LaHara: ha usato Kazaa, l'hanno condannata a pagare duemila dollari di multa.**

**D.: Per cui l'utente vede una pagina Web e poi clicca su un link per ricevere la musica via rete P2P.**

**R.**: *Esattamente, con tanto di contenuti multimediali che attraverso il Web sarebbe oneroso servire.*

---

**D.: Chi può partecipare a questa iniziativa?**

**R.**: *Chi vuole. Non costa niente. Non pensiamo nemmeno che costerà qualcosa in futuro.*

---

**D.: Ma come funzionerà?**

**R.**: *Ora il tipo di link appena descritto è poco conosciuto, ma nel prossimo futuro sempre più gente userà la Library di LimeWire. È un tipo di browser di file. Dentro l'applicazione LimeWire c'è una linguetta cliccabile "Library" dentro cui si vedranno i link a questi file speciali e i link a file condivisi contenuti in questo tipo di file. Si potrà spedire via email questo o quel pacchetto ad altri con un semplice clic e il client LimeWire partirà direttamente dal client email del destinatario.*

---

**D.: Per chi è LimeWire?**

**R.**: *È scritto in Java e quindi va bene per tutti.*

---

**D.: Quanti utenti avete?**

**R.**: *Abbiamo smesso di controllare da un po'. A un certo punto so che avevamo circa 300 mila utenti al giorno, a metà tra Windows e Macintosh.*

**Kurt Gödel**
**kurtgoedel@hackerjournal.it**

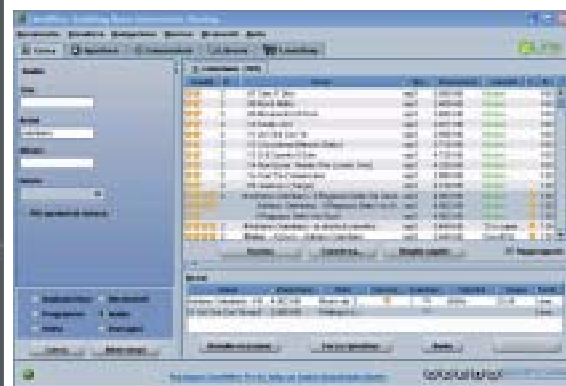
### alcuni siti per il peer-to-peer

| | |
|---|---|
| BitTorrent | http://bitconjurer.org/BitTorrent/index.html |
| Direct Connect | http://www.neo-modus.com |
| eDonkey | http://www.edonkey2000.com |
| Gnutella | http://www.gnutella.com |
| Kazaa | http://www.kazaa.com |
| LimeWire | http://www.limewire.com |
| LimeWire.org (sviluppo e community) | http://www.limewire.org |
| WinMX | http://www.winmx.com |

## TIPS

### QUALCHE CONSIGLIO DI P2P

Spesso pochi semplici trucchi aiutano lo scaricamento dei file sulle reti P2P. Eccone qualcuno.



**SCARICARE I FILE PIÙ IN ALTO NELLA LISTA**
Ordinando i file per "#" in LimeWire si ottiene il numero di host che dispongono di quel certo file. Più sono gli host, più è probabile che lo scaricamento andrà a buon fine.

**CHATTARE**
Oltre a conoscere, magari, persone interessanti, spesso fare due chiacchiere aiuta a farsi una cerchia di host affidabili da cui diventa più facile, se non piacevole, scaricare.

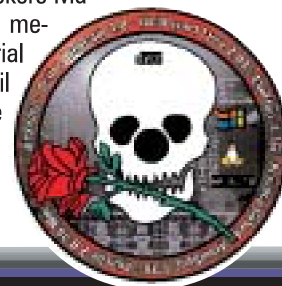
**CONDIVIDERE**
I vampiri sono quelli che pretendono di scaricare senza offrire niente in cambio. Spesso si ritrovano con un pugno di mosche…

**APPROFONDIRE**
In LimeWire il menu Tools -> Statistics permette di capire molte cose sul funzionamento interno di LimeWire e così aumentare il rendimento del programma.

---

### LIMEWIRE ON HACKERS MAGAZINE

Nel numero di Hackers Magazine di questo mese trovate un tutorial per usare meglio il programma e anche qualche sorpresa sul CD-ROM allegato. Non perdetelo!



# STRINGERE IL CERCHIO

**Tutti investigatori con le informazioni che la rete svela per noi. Abbiamo un solo indizio? Niente paura, gli siamo già addosso. Ma attenzione alla privacy.**

**"La ragazza si chiamava Chiara e l'ho persa di vista da parecchio tempo. Se gli anni maturano, adesso dovrebbe essere veramente carina, mi piacerebbe rivederla. Ma non ne conosco nemmeno l'indirizzo di posta elettronica".**
"Ho un'offerta di lavoro, ma la società che me l'ha proposta non so nemmeno cosa faccia, esattamente. Sarà affidabile? Eppoi era un'inserzione su Internet per andare in Francia. Sarà una bufala? L'unica cosa che mi rimane in mano è la loro partita Iva…"
"Ieri sera hanno abbandonato un'automobile proprio davanti a casa mia e oggi è ancora lì, ma non ha un bell'aspetto. Non sarà per caso rubata?"

## >> Piccoli investigatori crescono

Ciascuno di noi lascia una traccia, soprattutto se naviga in rete. E chi non lo fa? Per non parlare degli efficienti servizi che rendono la vita di tutti più comoda, più sicura, più completa e agevole. Non ci vuole molto a verificare un nome nelle pagine bianche (www.paginebianche.it). Un colpo di clic e otto volte su dieci abbiamo l'indirizzo, il telefono e spesso il tipo di attività della persona cercata. Ovunque in Italia. Come, l'attività? Dalla ragione sociale, s'intende, della piccola società da lui fondata. In fondo il nostro paese è o non è ricco delle piccole e medie imprese? Che appaiono ovviamente ben catalogate sotto lo stesso nome, perché nelle società di persone la ragione sociale contiene obbligatoriamente anche il nome del principale proprietario.
Ma non sempre è così facile. A chi sarà intestata la srl a cui dovrei pagare l'affitto? Chi è l'amministratore delegato? Non ho particolari elementi. Ma la cerco sulle pagine gialle (www.paginegialle.it). Potente, lo strumento. Peccato che oltre il telefono, l'indirizzo postale e una indicazione della email non mi restituisca più nulla. Di telefonare e chiedere dell'amministratore delegato non mi va. Inoltre dovrei lasciare i miei dati e saprebbero tutti che ho cercato informazioni su di loro. Meglio procedere per altre vie.
Prendo nota del dominio, appare così indifeso dopo la chiocciola dell'indirizzo email: info@dominio.it. Anzi, provo immediatamente a digitare nel browser www.dominio.it e poi anche .com. Nel novanta percento dei casi hanno almeno una paginetta sul web. E nel novanta percento dei casi pubblicano più informazioni di quante sarebbero necessarie. Annoto l'indirizzo e lo inserisco su www.viamichelin.com.
Che schifo, la zona è un groviglio di vecchi capannoni industriali, conosco il posto per via dei gruppi di amici che frequentavo una volta, quando più di un 125 non potevamo davvero permetterci.

Una ricerca sul servizio lycos per scovare qualche email: sempre meglio che niente.

## >> Ci siamo quasi...

Ok, proseguiamo. Devo capire chi è il boss, lì dentro. Un salto presso il RIPE (www.ripe.net) e gli dò in pasto il nome di dominio. Voilà. Come nel novanta percento dei casi, soprattutto




SPY-PH-NOKIA 8310

8310 - TELEFONO GSM MODIFICATO

Siamo in grado di modificare cellulari serie Nokia. Ad insaputa di chi li usa possono, se chiamati da un numero predefinito, trasformarsi in sensibilissimi microfoni ambientali. Apparentemente sono normalissimi telefoni cellulari, possono ricevere e chiamare in qualsiasi momento.
La distanza di trasmissione e' naturalmente illimitata.
Il microfono ipersensibile permette un ottimo livello di ascolto nel raggio di circa 4 - 5 metri.

E' infatti possibile programmare un numero di telefono chiamante. Quando SPY-PH riceve una chiamata da questo numero, automaticamente, e senza modificare il proprio aspetto visivo ed acustico, attiva un sensibilissimo microfono ambientale. Da quel momento SPY-PH e' in grado di trasmettere chiaramente tutti i suoni ambientali a distanza illimitata.

SPY-PH, inoltre puo' essere utilizzato come microspia INFINITY consentendo l'ascolto remoto in ogni momento. Lasciata inavvertitamente su un tavolo, durante un meeting d'affari, vi permettera' di controllare gli umori dell'uditorio, durante la vostra assenza.




COD.ART.:
SPY-PH-NOKIA 8310
>>> Info

**Attenzione! L'uso improprio di questi apparecchi è assolutamente proibito dalla legge.**

per queste piccole e medie società, il dominio è stato registrato presso l'Authority dando il nome dell'unico vero responsabile dell'azienda: l'amministratore delegato, appunto. Così adesso so esattamente come si chiama, ma anche il suo indirizzo di residenza. Preciso preciso. Trovare il suo telefono di casa abbiamo già detto che è un gioco da ragazzi. Ora so chi è, dove abita, di quale azienda… già, l'azienda. Ma cosa fanno lì dentro? Ne riprendo il nome e chiamo il sito delle Camere di Commercio

```
domain:     mathesis.de
descr:      Mathesis GmbH
descr:      Friedrichsplatz 11
descr:      68165 Mannheim
descr:      Germany
nserver:    ns1.manet.de
nserver:    sun0.urz.uni-heidelberg.de
status:     connect
changed:    20030317 104136
source:     DENIC

[admin-c]
Type:       PERSON
Name:       [redacted]
Address:    Mathesis GmbH
Address:    Friedrichsplatz 11
City:       Mannheim
Pcode:      68165
Country:    DE
Changed:    20030311 160948
Source:     DENIC

[tech-c]
Type:       PERSON
Name:       Domainverwaltung Manet GmbH
Address:    Manet GmbH
Address:    Luisenring 49
City:       Mannheim
Pcode:      68159
Country:    DE
Phone:      +49 621 3369 0
Fax:        +49 621 3369 334
Email:      domainverwaltung@manet.de
Changed:    20000710 121807
Source:     DENIC
```

**I dati registrati nei database dei domini sono una collezione di spunti interessanti.**



**Un altro buon punto di inizio per il data collecting di informazioni personali.**

(www.infoimprese.it) Due clic e leggo perfino l'estratto dello Statuto. Grandioso. Non mi avevano mai detto di avere un'attività primaria di import/export. Torno un attimo sul sito, magari trovo la lista delle referenze di qualche cliente. Eccola.
Ne prendo uno che sembra citato più volte, forse per loro è importante. Chi è? Un giro si tools-net.com e con lo stesso trucco già visto ho le info del mister che ha registrato il dominio. Provo a verificarne qualche caratteristica. Avrà pure, qualche volta, utilizzato ICQ… provo www.freeonlinepeoplesearches.com/email.htm. Tombola! E' uno di quelli che in rete ha lasciato tutto: recapito, interessi, età… bah, lascio la pista e vado dormire. Ormai s'è fatto tardi e domani deciderò cosa fare. Ne so abbastanza. E se appena potrò, gli regalerò un bel cellulare. Spia.
(www.endoacustica.co/telefonia).

**OneForBus**
**one4bus@hackerjournal.it**

# TIPS

## I SERVIZI PER SAPERE TUTTO, DI TUTTI

http://www.checkdomain.com/
whois per conoscere l'intestatario, la nazionalità, la città, la residenza, i numeri telefonici e i nominativi dei responsabili tecnici legati a un dominio Internet. Utile a completare i dati ottenuti da un risolutore di nomi di dominio o un tracer di indirizzi IP
Sicuramente da integrare con il database europeo http://www.ripe.net e quello italiano http://www.nic.it/RA/database/database.html

http://tools-on.net/
Un notevole insieme di servizi tra cui whois e molto altro, compresi alcuni elenchi di anonimizers.

http://www.infoimprese.it/
Tutto quello che vi può servire conoscere di un'impresa italiana. Per verificare l'esistenza, la posizione e l'indirizzo di una società (snc, sas, srl, spa). Verifica partita IVA, data di inizio attività, l'esistenza di eventuali sedi secondarie, l'attività dettagliata, i siti internet, gli indirizzi email, i numeri telefonici, il codice ISTAT, la ragione sociale esatta, le attività principali e secondarie e così via.

http://www.agenziaentrate.it/servizi/vies/vies.htm
Verificate dal numero della partita Iva l'esistenza di una società, in tutta europa.

http://www.planetsearch.com/
Un motore multiricerca. Avete solo una labile traccia? Iniziate da qui.

http://www.virgilio.it/servizi/computer/020.html
Potrebbe anche avere lasciato appositamente il suo indirizzo di email a un servizio dedicato. L'ingenuo.

http://coordinamento.mininterno.it/servpub/ver2/principale.htm
Targhe rubate, banconote false, documenti smarriti o rubati: tutto è registrato qui, potete verificarlo personalmente.

http://www.poliziadistato.it/bacheca/recuperati/recuperati.htm
Alla ricerca di qualche informazione su oggetti rubati? Qui sono perfino recuperati e fotografati.



Anno 2 - N. 40
18 Dicembre 2003- 1 Gennaio 2004

**Direttore Responsabile:** Luca Sprea

**I Ragazzi della redazione europea:**
grand@hackerjournal.it, Il Coccia, Gualtiero Bismark.it, Tronconi, Ana Esteban, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron

**Service:** Cometa s.a.s.

**DTP:** Cesare Salgaro

**Graphic designer:** Dopla Graphic S.r.l.
info@dopla.com

**Copertina:** Daniele Festa

**Publishing company**
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

**Printing**
Roto 2000

**Distributore**
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

**Abbonamenti**
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.



**HJ: INTASATE LE NOSTRE CASELLE**
Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. **redazione@hackerjournal.it**

## hack·er (hãk'∂r)

*"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."*

# LUCY IN THE SKY WITH FUNCARD

Per chi fosse di ritorno ora da un viaggio sulla Stazione Spaziale Internazionale (http://spaceflight.nasa.gov/station), da qualche tempo nel panorama della TV satellitare italiana è arrivata la Sky di Rupert Murdoch a prendere il posto di Tele+ e compagnia.

Contemporaneamente nei forum e nei newsgroup è scoppiato un bel pandemonio. Se prima lo sport preferito degli italiani-con-parabola era trovare il modo di guardarsi le partite a scrocco o ridiffondere per tutto il condominio il segnale di un singolo decoder, ora la cuccagna sembra finita. Sky ha sistemi di cifratura più astuti e flessibili, si dice, e piratare le sue card è divenuto impossibile oppure molto meno facile e conveniente di prima, si dice.

Detto che non esista alcuna protezione inviolabile, il problema è trovare un modo semplice e praticabile per violarla e questa sembra essere la situazione attuale. Abbiamo fatto il punto della situazione e anche dato un paio di avvisi ai naviganti più sprovveduti, perché c'è gente che va in giro a millantare credito per estorcere denaro ai gonzi, e là fuori è pieno di gonzi (la prova è che i lettori di Hacker Journal sono decine di migliaia e gli italiani sono decine di milioni. I gonzi sono tutti fuori dal primo insieme e dentro il secondo :-)

Torneremo sull'argomento anche perché tra poco arrivano i decoder digitali terrestri e il tutto diverrà ancora più interessante. È proprio bello vivere in tempi di continue novità tecnologiche!

Come si noterà, abbiamo lavorato a un bel restyling della rivista. Speriamo che piaccia e restiamo in attesa di complimenti e critiche, in modo da creare un Hacker Journal più che mai all'altezza di tutte le aspettative.

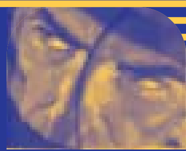
Sky non è certo l'unica attrazione di questo numero, peraltro; parliamo di X-box contro Linux, tecniche base di ingegneria sociale, bambine dodicenni condannate a pagare duemila dollari di multa per avere usato un programma peer-to-peer e altro ancora, passando per tutorial e cose di imparare pensate un po' per tutti.

Tra questi ne segnaliamo uno in particolare, quello dedicato a Google. È accessibile a chiunque ma contiene qualche dritta anche per i più bravi. Se c'è uno strumento che sembra veramente universale di questi tempi, è proprio il motore di ricerca, e il motore di ricerca, insomma, è Google.
Buona lettura e sotto con l'hacking!

**Barg the Gnoll**
gnoll@hackerjournal.it

**One4Bus**
one4bus@hackerjournal.it

# NEWS



## NEWS

### ■ CARTE D'IDENTITÀ BIOMETRICHE: INUTILI?

Il Regno Unito sta pensando di introdurre carte di identità biometriche che riportano dati considerati praticamente non falsificabili, come scansioni della retina e altro. Tuttavia le analisi della London School of Economics mostrano come il sistema progettato non fermerà i criminali intenzionati a procurarsi più carte sotto nomi diversi. In più la scansione della retina è un procedimento ancora troppo soggetto a fattori ambientali, tanto che il riconoscimento ha una precisione del 99 percento. Sembra molto alta e invece, su database enormi come quelli di una popolazione nazionale (si pensi all'Italiam con 60 milioni di abitanti) è una percentuale disastrosamente bassa, che arrecherebbe grandi fastidi a cittadini onesti e aumenterebbe le probabilità che un criminale la faccia franca. Si stanno studiando soluzioni come quella di includere nella carta sia la scansione retinica sia l'impronta digitale. La precisione aumenterebbe di molto, ma così anche i costi.

---------------------------------------

### ■ SCRIVI, SCRIVI, CHE TI PARAFRASO

Tutti i giorni riformuliamo un sacco di volte il nostro pensiero, per rispiegare una cosa che il nostro interlocutore non ha capito, oppure per portare un attacco vincente di ingegneria sociale verso un ignaro impiegato dei telefoni o delle poste. Questa è una cosa che da sempre ci distingue rispetto ai computer, incapaci di parafrasare alcunché.
Le cose però iniziano a cambiare. Un team di ricercatori della Cornell University ha mutuato procedure tipiche del giornalismo online, le ha incrociate con schemi di analisi tipici della bioinformatica ed è arrivato a progressi sostanziali in materia.
In pratica i ricercatori hanno studiato come più persone esprimono in parole diverse lo stesso concetto e hanno confrontato i vari modi di espressione con tecniche usate normalmente per confrontare tra loro i geni che albergano nel DNA.
Dopo Google News, che raccoglie le notizie automaticamente, sta arrivando dunque il redattore elettronico, capace di riassumere e rielaborare le notizie da solo. Mi sa che nel 2015 Hacker Journal lo scriverà un computer Linux, tutto da solo. O no?

## ➲ 29 NOVEMBRE: VIVA IL SOFTWARE LIBERO!




Grande attività e tanti incontri in tutta Italia per la giornata nazionale del software libero, celebrata sabato 29 novembre scorso. Non abbiamo lo spazio per raccontare tutto ora (qualcuno ha voglia di rassumerci le sue esperienze personali?) ma di città in città si sono moltiplicate le iniziative di ogni genere di associazioni. Dopo i 40 Comuni coinvolti dell'edizione 2001 e i 60 del 2002, si può solo parlare di ennesimo record. Per fare solo qualche esempio, a Milano il Laboratorio Innovazione Breda ha visto oltre mille visitatori. A Firenze l'incontro è stato dedicato al software libero nei Paesi in via di sviluppo, organizzato dal Firenze Linux User Group. A Trento si è parlato di tutto, dalle distribuzioni più recenti alle esperienze dei nuovi arrivati. A Crema si parlato di tutto, dalle sottigliezze tecniche del kernel fino al rapporto tra Linux e videogiochi. E così via. Attendiamo i resoconti da tutta Italia per dare loro il massimo spazio possibile su Hj!

http://milano.linux.it
http://www.firenze.linux.it
http://www.linuxtrent.it
http://carapax.crema.unimi.it/eventi/ld2003/ld2003.php

## ➲ FINE DI (ALMENO UN) DIALER

Ha fatto la fine che si meritava il finto notiziario Inforete, che con la scusa delle news in realtà portava a un dialer per spillare soldi ai navigatori più ingenui dall'indrizzo http://members.yodahosting.com/inforete. Di dialer ce ne sono milioni ma questo aveva veramente esagerato, copiando informazioni da Punto Informatico per sembrare più attendibile. Se il pericolo esisteva solo per chi usa Windows insieme a Internet Explorer (la combinazione più esposta a dialer e vari altri tipi di codice ostile presente sul Web), è comunque confortante sapere che il sito è stato disattivato. In questo momento all'URL si può vedere un commento poco gentile di "hacker poco pazienti" e niente più. bene così.

**Attacco portato da hackers non pazienti**

The Doc on The Rock.

## ➲ UN ALBERO DA HACKER

È Natale per tutti, anche per chi vede le cose con occhio diverso dagli altri e inventa utilizzi nuovi per le cose vecchie: come dire un hacker.
E allora, chi più hacker di Pietro Cucchi, imprenditore di Bussero (alle porte di Milano), che ha voluto un albero di Natale artificiale alto oltre cento metri, addobbato da non meno di 237 mila lampadine.
A metà tra l'attrazione turistica e il capolavoro postmoderno, l'albero è sostenuto da una struttura esagonale in acciaio del peso di oltre quindici tonnellate. Le luci sono gestite da un software apposito che crea combinazioni di luci sempre nuove.
Se passate da Bussero, in via Genova 2, avete tempo fino al 16 gennaio 2004 per vederlo dal vivo. Nel frattempo consideratelo come un piccolo grande augurio di Natale per tutti i lettori di Hacker Journal e, già che ci siamo, anche Hackers Magazine.






## GLI USA DI NUOVO VERSO LA LUNA?

Da anni il programma spaziale americano procede ma ha perso molto dello spunto iniziale che ha portato Neil Armstrong a sbarcare per primo sul nostro satellite. Problemi finanziari, incidenti mortali alle navette Challenger e Columbia e scarsa efficienza di molti enti hanno infatti ridotto le aspettative e le prospettive dei programmi spaziali della NASA.
Tutto questo potrebbe però cambiare il 17 dicembre, quando il presidente George W. Bush terrà un discorso in occasione del centenario del primo volo umano a bordo di un mezzo più pesante dell'aria. Secondo molti, infatti, Dubya (il nickname di Bush figlio) sceglierà proprio quell'occasione per rilanciare il sogno della conquista spaziale, finito in soffitta da oltre trent'anni. Dopo l'epico sbarco del 21 luglio 1969, infatti, le missioni lunari hanno avuto luogo fino a dicembre 1972, per poi terminare. A oggi più di 125 milioni di americani sono nati dopo che l'ultimo uomo ha posato l'ultimo piede sulla Luna.
Violare i computer della NASA potrebbe tornare a essere uno degli sport preferiti degli hacker più intraprendenti.



**La Luna, come in questa foto spettacolare, si è eclissata. Ma forse ci torneremo.**

## HP SI SVEGLIA SULLA MUSICA ONLINE

Hewlett-Packard si è improvvisamente svegliata da un lungo sonno e ha deciso di lanciare un negozio online di musica entro il primo trimestre del 2004. Secondo Peter Appl, amministratore delegato di HPShopping.com, il servizio di vendita online avverrà in collaborazione con un'iniziativa già esistente, come Musicmatch.com. Inoltre la società lancerà sul mercato un riproduttore portatile di musica digitale.
HP è il secondo produttore mondiale di computer dopo Dell, ma sulla musica online è come se fosse ultima. Il mercato, infatti, è dominato dall'iTunes Music Store di Apple (che si dice arriverà a maggio anche in Europa) e dall'analogo servizio di Dell, con dietro numerosa concorrenza che arranca. Al tempo stesso, Apple con il suo iPod e Dell con il suo Digital Jukebox, alias DJ, dominano qualsiasi classifica di vendita di player musicali da taschino.
HP è grande; magari ha anche qualche grande idea per scalzare i numeri uno attuali. Sarà meglio che sia così, perché anche l'idea giusta fa un sacco di fatica i più quando è messa in atto nei tempi sbagliati.




## UN PUZZLE DA VERI HACKER

Mille pezzi, cinquemila pezzi, settemila pezzi sono roba da niente.
Pensate a un puzzle dove i pezzi hanno tutti forma uguale e ci sono miliardi di incastri possibili ma una sola soluzione corretta.
È il principio dello Shmuzzle, gioco inventato da tale Sam Savage, già docente di Management Science alla Università di Chicago. Savage ha avuto l'idea osservando alcune opere di Maurits Cornelis Escher, artista olandese morto nel 1972 e autore di lavori che nascondono trame geometriche assai intricate e paradossi della prospettiva che lasciano interdetti.Escher era un maestro della tassellatura, l'arte di riempire completamente un piano con figure che si incastrano l'una nell'altra all'infinito, senza lasciare spazi vuoti.
E da un'opera di Escher intitolata Reptiles è nata l'idea di creare un puzzle dove lo scopo è sempre quello di comporre il disegno, ma i pezzi hanno tutti forma uguale.
Invitiamo tutti a fare un salto su http://www.shmuzzles.com, dove è anche possibile provare l'ebbrezza di un puzzle davvero impossibile direttamente da browser.
Il vero hacker si fermerà anche a considerare i principi geometrici che stanno dietro al lavoro, magari aiutandosi con http://www.shmuzzles.com/formula.htm.

NEWS

## MAI PIÙ SEDIE A ROTELLE

All'università Waseda di Tokyo, in collaborazione con la produttrice di robot Tmsuk, i ricercatori hanno messo a punto un prototipo di robot capace di camminare su due gambe meccaniche e contemporaneamente trasportare una persona seduta. Si può immaginare come un progresso di questo tipo spalanchi la porta a un futuro assai più confortevole per i disabili e gli ammalati. Il prototipo si chiama WL-16, è alimentato a batterie e riesce a spostarsi in avanti, all'indietro e lateralmente reggendo un adulto del peso massimo, per ora, di sessanta chili. Secondo Yoichi Takamoto, amministratore delegato di Tsmuk, per arrivare a un modello realizzabile in serie ci vorranno "almeno due anni". Nel frattempo, però, il robot è già capace di mantenere l'equilibrio quando il suo carico umano si sposta e riesce a fare passi lunghi trenta centimetri. Prossimi obiettivi: renderlo capace di fare le scale (per ora il gradino massimo superabile è alto pochi millimetri) e passare dall'attuale radiocomando a un joystick montato a bordo, utilizzabile dal passeggero.

## SUN ATTACCCA MICROSOFT CON JAVA LOW-COST SU LINUX

Nell'intento di togliere quote di mercato a Windows nel mondo aziendale, Sun ha abbassato il prezzo del suo Java Enterprise System a 50 dollari l'anno per utenza e ha portato Java Desktop System, che consente di collegarsi a un ambiente Windows da una interfaccia interamente basata su Linux con Star Office e Ximian, a 25 dollari per utenza per anno, il tutto fino a metà 2004.La mossa segue il successo conseguito da Sun in Cina, dove un accordo con China Standard Company, azienda controllata dal governo cinese, apre la strada letteralmente a centinaia di milioni di computer sui quali verrà installato Java Desktop System e non Windows.

# NEWS

## NEWS

## CISCO VULNERABILE SUL WI-FI

Cisco, monopolista di fatto del mercato dei router, ha ammesso recentemente una vulnerabilità nella sua linea di punti di accesso wireless Aironet che può consentire ad aggressori ben motivati di accedere a una rete aziendale e curiosare oltre il lecito. Il problema sta nelle chiavi di cifratura, che vengono trasmesse in modo wireless e in testo non cifrato: quindi chiunque, dotato di un computer e dell'antenna giusta, può intercettare le chiavi stesse. una volta che un aggressore è in possesso delle chiavi, qualunque cifratura è inutile per proteggere i dati.



La vulnerabilità affligge i modelli delle serie 1100, 1200 e 1400 con software Cisco IOS 12.2(8)JA, 12.2(11)JA e 12.2(11)JA1. Gli amministratori di rete possono risolverla, tra l'altro, aggiornando a IOS versione 12.2(13)JA1 o successivo. Certo che se gli aggiornamenti fossero numerati in modo più umano anche le vulnerabilità avrebbero vita più difficile!
http://www.cisco.com/warp/public/707/cisco-sa-20031202-SNMP-trap.shtml

---

## UN HOTSPOT IN OGNI BIBLIOTECA… MA IN INGHILTERRA

Il ministro inglese Stephen Timms ha aperto il lavori di un convegno su Wi-Fi & 3G confermando che va avanti il piano di installazione di un punto di accesso wireless in ogni biblioteca pubblica del Regno Unito, annunciato lo scorso settembre. Si spera che i nostri governanti, se non sanno fare meglio, almeno siano in grado di scimmiottare i colleghi britannici.

## VELOCE COME LA LUCE

Da Israele proviene il processore più veloce del mondo, che sfrutta la luce invece della corrente elettrica (www.lenslet.com). Il che significa che è capace di elaborare qualcosa come 8 mila miliardi di operazioni ogni secondo (8 TeraOPS), stracciando di oltre mille volte in velocità qualunque altro dispositivo di elaborazione dei segnali attualmente in commercio.
Il responsabile della Ricerca e Sviluppo del Ministero della Difesa dell'esercito israeliano ha affermato che "Un tale salto quantico nelle prestazioni computazionali, dovuto all'elaborazione ottica, apre nuove possibilità negli scenari militari del futuro, con rilevanti implicazioni strategiche. Questo nuovo sviluppo rivoluzionerà la natura stessa del modo di fare guerra, con effetti simili a quelli che vennero causati dall'introduzione delle navi o degli aeroplani…". E se lo dice lui…
Le applicazioni più probabili di questo Digital Signal Processor saranno infatti nel settore della difesa (crittografia, elaborazione dei dati grafici provenienti da sistemi satellitari, riconoscimento automatico di forme, eccetera) e nell'ambiente multimediale e della comunicazione. E potete già immaginarvi cosa accadrà alla TV: la trasmissione di immagini video ad alta risoluzione a compressioni fantastiche vi porterà in casa una impressionante scelta di canali. Ma c'è chi sta già cercando di applicare il processore ottico alle nuove consolle, per giocare a velocità mai viste …



## IL GRANDE FRATELLO PASSA PER LE MUTANDE

Radio Frequency IDentification: passa da questa sigla la morte dei codici a barre e la nascita dello spyware nelle mutande. C'è gran fermento nelle associazioni dei consumatori americani: prevedono la sostituzione dei codici a barre associati ai barattoli della marmellata e agli altri prodotti da supermercato con etichette 'attive'. In grado, quindi, di inviare dati di prezzo, quantità e tipologia di prodotto direttamente ai ricevitori posti alle casse.




**Maxell ha sviluppato un chip RFID notevolmente piccolo, piazzando l'antenna direttamente sulla superficie del chip. Robustezza, affidabilità e... occultamento sono garantiti.**

Non solo si avvicina la scomparsa delle cassiere, ma soprattutto si teme che qualche azienda di produzione dei vestiti possa inserire il chip direttamente nel tessuto. Sarebbe così possibile capire quante volte il cliente torna in negozio, o perfino quali e quanti negozi va a visitare. Al di là dei poco ortodossi fini commerciali, significa in sostanza poter tracciare facilmente tutti gli spostamenti di una persona, in sostanza ogni volta che esce da casa.
C'è anche chi sostiene che ad un'etichetta del genere sia possibile associare un numero identificativo unico e personale, valido universalmente. Una sorta di tracciatore che, se occultato, porterebbe veramente alla scomparsa del gioco di nascondino.
Peraltro molte ricerche di mercato non danno RFID come uno standard facilmente utilizzabile, ma in Europa la catena di grande distribuzione Metro è in fase di avanzata sperimentazione delle etichette RFID, così come Wal-Mart e Marks&Spencer negli Stati Uniti.
Tutti concordano, peraltro, che sarebbe prima necessaria una legislazione adeguata, che porti a dei limiti di utilizzo dei chip RFID se questi intaccano la privacy delle persone 'normali'. Ma si sa: fatta la legge, e con la tecnologia giusta...

